American Water Works Association

The Authoritative Resource for Safe Drinking Water℠

PROTECTING OUR WATER

Drinking Water Security in America After 9/11

Advocacy
► *Communications*
Conferences
Education and Training
Science and Technology
Sections

American Water Works Association

The Authoritative Resource for Safe Drinking Water℠

6666 West Quincy Avenue
Denver, CO 80235-3098
T 303.794.7711
F 303.794.7310
www.awwa.org

Advocacy
Communications
Conferences
Education and Training
Science and Technology
Sections

Dear Friends:

As our nation forges ahead in this new era of homeland security concerns, multiple sectors have been affected. Drinking water in particular continues to be a critical component of national security, as millions of Americans rely on their local water utility to provide safe and affordable drinking water. This report highlights what the drinking water profession has done to secure the nation's water supply, both before and after the attacks of September 11, 2001, as well as the challenges that lie ahead.

The American Water Works Association (AWWA) is proud to represent a profession so committed to the safety of its customers. This report provides a clear understanding of the actions taken by utilities, Congress, USEPA, and even consumers to ensure that our nation's water supply remains safe and secure.

The state of our nation's water supply detailed in this report demonstrates that water utilities are rethinking how they approach security and are developing a never before seen culture of security within the profession. There is much still to be done, but there is also much to be proud of.

Sincerely,

Jack W. Hoffbuhr, P.E.
Executive Director
AWWA

PROTECTING OUR WATER

Drinking Water Security in America After 9/11

Introduction

The terrorist attacks September 11, 2001, brought a new era to American water utilities. Although drinking water in the United States has long been recognized as among the safest in the world, the devastating events of that day brought water security to the forefront as a priority. Since then the security of America's water supply has been a paramount concern to the Environmental Protection Agency (USEPA), to water utilities, and to the associations that represent and serve them.

This report summarizes the actions undertaken by the drinking water community, in partnership with USEPA and others, to help secure America's water supply against terrorist attack. It also identifies some of the challenges ahead. Obviously, it would be inappropriate for this report to provide information or details that could themselves compromise the security of America's water supply, so by design, it is brief and, in some cases, nonspecific.

Executive Summary

The drinking water community, in partnership with USEPA and others, actually began to prepare for terrorist threats before September 11, 2001. In 1998 President Clinton signed Presidential Decision Directive 63 and thereby identified water as one of America's critical infrastructures. Under that Directive, USEPA was assigned lead responsibility for the water sector and, in turn, designated the Association of Metropolitan Water Agencies (AMWA) as the lead for this sector. At the same time, the American Water Works Association (AWWA) began to prepare technical materials and publications for water utilities relating to water system security. These efforts went into high gear immediately after the terrorist attacks on New York and Washington. Since then, AWWA has held workshops and training sessions around the country, reaching over 2,500 water systems with seminars, training, videos, and technical assistance. AMWA has developed and launched a secure information system for water utilities known as the WaterISAC. Individual utilities have developed

vulnerability assessments and emergency response plans. And USEPA has published important information for utilities and provided financial and other support. These activities accelerated with the passage of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (PL 107-188, commonly called the Bioterrorism Act).

Taken together, this mobilization of effort and resources is virtually unprecedented. It has resulted in the development of the following:

Results of Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (PL 107-188)

- USEPA's "Baseline Threat Report" describing likely modes of terrorist attack and outlining the parameters for vulnerability assessments by community water systems. This is sensitive information, provided only to water utilities;
- Risk assessment tools for utilities to identify and evaluate their own security risks. Such analyses, called vulnerability assessments, are required by the Bioterrorism Act;
- Training programs on vulnerability assessments, used by several thousand water systems, to help utilities prepare accurate and detailed assessments;
- Security protocols to assure that vulnerability assessments are safeguarded after they are sent to USEPA, as required by the Bioterrorism Act;
- Guidance and technical assistance for utilities to use in revising emergency response plans as required by the Bioterrorism Act;
- Development of information on "best practices" and technical assistance on matters such as security hardware technologies;
- An inventory of past security threats to community water systems and the lessons learned from them;
- Analysis of the lessons learned by community water systems through the vulnerability assessment process;
- Guidelines that water utilities may use to guard against terrorists and security threats, correlated with the Department of Homeland Security's color-coded advisory system; and
- The Water Information Sharing and Analysis Center (WaterISAC), which provides a secure portal for the communication of sensitive security information among utilities, law enforcement, and intelligence agencies.

A recent survey sponsored by AWWA and AMWA identified 86 items in the current inventory of security products and services for water utilities. Most of them have been developed through the mobilization of water community and USEPA resources since 9/11. Most important, the survey found that most utilities perceived these tools to be of high value. This inventory of tools is available on the AWWA Web site (www.awwa.org).

By working together in a constructive partnership, water utilities and USEPA have accomplished much in a relatively short time. Everyone has a critical role in this process. Utilities are conducting vulnerability assessments, revising their emergency response plans, and installing and maintaining security improvements. They are also instilling a strong culture of security throughout the water community to ensure that these new security policies and procedures are effectively implemented over the long term. The associations that represent and serve the water community are reaching out to utilities, providing training and technical assistance, offering new programs, and developing new tools to enhance the security of America's water supply.

USEPA has an important role to play as well. The development of guidance, new analytical tools, research, and financial assistance are important federal responsibilities.

Finally, the public has an important role in safeguarding the security of our water supply. In many cities and small towns, the public is the first line of defense, serving as an extra set of eyes watching over key utility assets such as tanks, reservoirs, and even fire hydrants.

The collaboration since September 11, 2001, on water security has been unprecedented. While America's water systems were safe to begin with, utilities, the public, and the federal government have worked hand-in-hand to make them even safer. While more work is left to be done, by continuing to work together we can keep America's water supply the safest in the world.

Chapter 1— The Bioterrorism Act

When President Bush signed the Public Health Security and Bioterrorism Preparedness and Response Act into law last June, water utilities entered a whole new realm of emergency preparedness. Title IV of the Bioterrorism Act amended the Safe Drinking Water Act (SDWA) and mandated specific actions to improve water security, with specific deadlines and requirements for both water utilities and USEPA.

The Bioterrorism Act mandated five new security requirements for all community water systems serving more than 3,300 people. Collectively these aproximately 8,000 utilities serve over 240 million people, or about 90 percent of the nation's population served by community water systems.

Six months after submission of the vulnerability assessment, utilities are required to certify to USEPA that they have developed or revised an emergency response plan based on the results of the vulnerability assessment.
Under the Bioterrorism Act, both vulnerability assessments and emergency response plans have to focus on terrorist attacks or other *intentional* acts intended to disrupt the ability to deliver a safe and reliable supply of drinking water or otherwise present a significant health concern. This stands apart from the assessments and plans that most utilities have had in place for years in order to deal with natural disasters, vandalism, etc. While the assessments and plans that existed before September 11, 2001, may serve as a good starting point, the focus of the Bioterrorism Act is purposeful destruction or contamination, and water utilities must alter their emergency response plans to meet these new threats.

USEPA has its own set of deadlines in the Bioterrorism Act. Congress required that by August 1, 2002, USEPA would complete a baseline threat report with information on likely threats for utilities to consider in the development of a vulnerability assessment. USEPA completed the *Baseline Threat Information for Vulnerability Assessments for Community Water Systems* and provided this sensitive report to water utilities in the fall of 2002. The law also required USEPA to develop a protocol for protection of the submitted vulnerability assessments by November 30, 2002. In response USEPA has completed a protocol with multiple levels of protection to safeguard vulnerability assessments in a controlled-access facility at USEPA headquarters. USEPA is also required to conduct research on prevention, detection, and response to contamination and supply disruption, and a plan is under development. Finally, the law requires USEPA to develop guidance for small systems serving less than 3,300 people. While these systems are not required to conduct a vulnerability assessment and revise an emergency response plan under the Bioterrorism Act, many are implementing plans to protect their customers.

Virtually all of the largest utilities — those with the earliest deadline of March 31, 2003— submitted their vulnerability assessments to USEPA on or before the deadline. They are now revising their emergency response plans to reflect what they learned in the vulnerability assessment. Medium and smaller-sized utilities across the nation are in the process of developing their own vulnerability assessments, and they too will develop or revise effective emergency response plans. Both the utility community and USEPA are giving security the serious attention it deserves.

Bioterrorism Act Requirements

Community water systems serving more than 3,300 people are required to do the following:

1. Conduct a vulnerability assessment;
2. Certify to USEPA that the vulnerability assessment was completed by a date specified in the law;
3. Submit a paper copy of the assessment to USEPA;
4. Prepare or revise their emergency response plan based on the results of the vulnerability assessment; and
5. Certify to USEPA that the emergency response plan has been developed or revised by a date certain.

Deadlines for submission of vulnerability assessments to USEPA depend on the size of the water system:

- Systems serving more than 100,000 people–March 31, 2003
- Systems serving between 50,000 and 100,000 people–December 31, 2003
- Systems serving between 3,300 and 50,000 people–June 30, 2004.

Chapter 2— Vulnerability Assessments and Emergency Response Plans

Vulnerability Assessments

Vulnerability assessments are designed to help drinking water utilities evaluate their susceptibility to terrorism or other intentional acts that could harm public health or disrupt the water supply and to identify corrective actions that reduce or mitigate the risk of serious consequences. The processes for assessing such security risks have been evolving in recent years as threats have changed and as new security technologies have been developed.

In conducting vulnerability assessments, utilities must examine and consider the risks and identify countermeasures for a terrorist attack involving all the components of the water system.

This includes:

- Pipes and constructed conveyances;
- Physical barriers;
- Water collection, pretreatment, and treatment;
- Storage and distribution facilities;
- Electronic, computer, and other automated systems;
- The use, storage, and handling of hazardous chemicals; and
- The operation and maintenance of the system.

A number of security risk assessment procedures or tools have been developed and may be used to address the water system components identified above. However, many experts consider the tool known as RAM-W℠ to be the "gold standard" for developing water system vulnerability assessments for a number of reasons. It was generally used by the largest water systems due to its description in the USEPA grant application for financial assistance and because it is considered by many to be the tool that most lends itself to a long-term culture change in the utility. The AwwaRF and Sandia National Laboratories developed RAM-W℠ with support from USEPA, in late 2000–2001. AWWA and other organizations then undertook an extensive effort to train utilities in the use of RAM-W℠ throughout 2002 and early 2003. RAM-W℠ training is an intensive three-day class, with a mix of lectures and hands-on exercises. The participants typically use information provided by one of the water utility participants for the hands-on exercises so that they get the experience of working with real-world information. AWWA, as a licensed RAM-W℠ trainer, has conducted 22 training classes across the country for more than 1,200 participants to date. More training workshops are in development. Participants in these workshops include both utility personnel, who will use the method directly, and consultants or others who will use the method to assist utilities in the development of a vulnerability assessment.

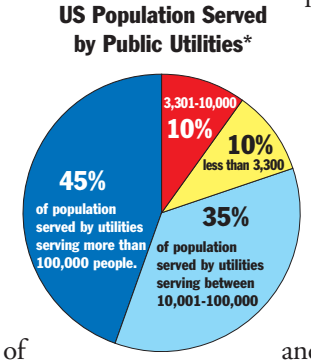
RAM-W℠ training workshops

RAM-W℠ and other vulnerability assessment tools are rigorous, thoughtful processes that, once completed, will tell a utility a great deal about its security. Using this method or one of a number of others, a water utility will undertake the following steps to assess its vulnerabilities to terrorist attack:

1. Characterize the water system, including its mission and objectives;
2. Identify and prioritize adverse consequences to avoid;
3. Determine critical assets that might be subject to malevolent acts that could result in undesired consequences;
4. Assess the likelihood (qualitative probability) of such malevolent acts from adversaries;
5. Evaluate countermeasures; and
6. Analyze current risks and develop a prioritized plan for risk reduction.

A good vulnerability assessment is not quick, and it is not inexpensive. Depending on its size and complexity, a utility will typically require several months and spend hundreds of thousands (in some cases, millions) of dollars to complete the vulnerability assessment. Virtually all utilities consider it time and money well spent.

Emergency Response Plans



After they complete a vulnerability assessment, water utilities are required by the Bioterrorism Act to prepare or revise an emergency response plan based on the results of the vulnerability assessment. Like the assessment, the emergency response plan focuses on terrorist or other intentional acts, in distinction to plans that most utilities have had for years for dealing with natural disasters. Utilities are not required to submit their emergency response plans to the USEPA, but they must certify to USEPA that they have completed the plan within six months after they send their vulnerability assessment to the Agency.

These new or revised emergency response plans differ substantially from traditional emergency plans for several reasons. Most traditional emergency response plans are developed to respond to a natural event, such as a hurricane, tornado, or earthquake, or an event such as a major water main break. In such events, the event itself is immediately apparent.

In some cases of a terrorist attack, the malevolent attack will also be immediately apparent. For example, explosives could be used to damage a utility's facilities and disrupt its operations. Existing water treatment chemicals, could be targeted to cause a deliberate release. Emergency response plans developed under the Bioterrorism Act have to be designed to prevent, mitigate, and respond to such events.

In other cases of a terrorist attack, the malevolent event may not be immediately apparent, and emergency response plans for terrorism have to be designed for these events as well. For example, the first indications of an attack using chemical or biological contaminants in a water distribution system could be an increase in taste or odor complaints by customers. In the worst case, the first indications of contamination in the distribution system could be an increase in emergency room visits. In such cases, utilities may have to make critical decisions almost immediately based on limited information. The new or revised

* Safe Drinking Water Information System/Federal version (SDWIS/FED) 02Q4

emergency response plans required by the Bioterrorism Act need to provide a framework for making such decisions.

Likewise, telling the public what to do may be quite different after a terrorist attack than after a natural disaster. For example, the recommended action after a natural disaster or major main break is often a "boil water" order. Such an order protects against gastrointestinal illness if bacteriologically contaminated water is used for drinking or cooking. Such water may generally still be used for bathing and other uses. During a contamination event, on the other hand, the agent in question may be unknown for a period of time. In that interval, the prudent public health response might be a "do not use"order.

Finally, the new or revised emergency response plans being developed in response to the threat of terrorism have to recognize that in the event of an attack, important parts of the utility would almost certainly be considered a crime scene. Utilities must be prepared to recover and operate without hindering a criminal investigation that may take some time to complete.

In another example of the unprecedented partnership between the drinking water community and USEPA, we are now working together to outline a decision-making and response process for the first few critical hours after an attack. Terrorism requires new tools, and working together, the drinking water community and the USEPA are responding.

Chapter 3— WaterISAC

With Presidential Decision Directive 63 and Executive Order 13231, Presidents Clinton and Bush designated the water sector and certain sectors of industry as critical to the country's well-being. These presidential decrees also called for the critical sectors to establish Information Sharing and Analysis Centers, or ISACs, to promote the exchange of security information.

Information Sharing and Analysis Centers, or ISACs, to promote the exchange of security information

The Association of Metropolitan Water Agencies (AMWA) is the private sector lead for the water sector. With initial funding for development from USEPA, the WaterISAC became operational in December 2002 for both drinking water and wastewater utilities. Long-term funding for the WaterISAC will come from

The WaterISAC will provide a wide array of information and tools to assist in identifying and assessing threats and in taking measures to mitigate those threats. The WaterISAC will also analyze incident reports and provide an important link between the water sector and federal homeland security, intelligence, law enforcement, environmental and public health agencies.

The WaterISAC provides the following products and services:

- Alerts on potential terrorist activity;
- Information on water security from federal homeland security, intelligence, law enforcement, environmental, and public health agencies;
- A database on chemical, biological, and radiological threats;
- Information on physical vulnerabilities and security solutions;
- Research, reports, and other information;
- Notification of cyber vulnerabilities and other technical fixes;
- A secure means for reporting security incidents;
- Vulnerability assessment tools and resources;
- Secure electronic bulletin boards and chat rooms on security topics; and
- Information on emergency preparedness and response resources.

While the analysis of incident reports and other intelligence is a critical function of the WaterISAC, it also provides a forum for the building of a security community within drinking water and wastewater utilities. Secure electronic bulletin boards and chat rooms will allow utility personnel to share important intelligence and talk about lessons learned from conducting vulnerability assessments and developing or revising emergency response plans. As such, the WaterISAC is an indispensable tool for dissemination of sensitive security information among water utilities, law enforcement, and intelligence agencies.

Chapter 4— The Current State of the Nation's Water Security

America has long enjoyed the safest drinking water in the world and among the lowest rates of waterborne disease of any nation. Indeed, the Centers for Disease Control has said that waterborne disease is virtually undetectable in the health statistics of the United States. With respect to terrorism, most experts consider the likelihood of a successful terrorist attack on America through the water to be small. However, attacks against water systems are a known *modus operandi* of several terrorist groups. Materials relating to American water supply have been recovered from terrorist sites overseas. A damaging attack could affect water

quality and public health, or it could involve water supply, affecting fire control, sanitation, and so forth. Clearly, water supply is critical to homeland security. We are not invulnerable to terrorism, and the consequences of a successful attack through the water could be catastrophic.

Recognizing the critical importance of water to America's homeland security, drinking water utilities have been working hard to meet the mandates of the Bioterrorism Act. Over 400 of the largest US water systems, those serving more than 100,000 people, were required to submit a copy of their vulnerability assessment to USEPA by March 31. Collectively, these large systems serve about 120 million people, over 45 percent of the nation's population served by community water systems.

Although the deadlines in the Bioterrorism Act were very tight, it was apparent as of mid-April that the vast majority of water systems serving 100,000 people or more had completed their vulnerability assessments by their deadline. We are proud that virtually all the largest water systems have met that challenge. Those systems are now working on the development or revision of their emergency response plans.

Water systems serving between 50,000 and 100,000 people have until December 31, 2003, to submit their vulnerability assessments. There are approximately 500 such systems, and although there has been no direct survey of each one, we believe they are currently working hard to complete their vulnerability assessments, or have already done so. Likewise, evidence also suggests that medium-size and smaller utilities, those serving between 3,300 and 50,000 people, will meet their deadline for developing a vulnerability assessment. The evidence for this comes from limited samples of water utilities and from the fact that interest in vulnerability assessment materials, training, and technical assistance remains high among utilities of all sizes. Further evidence of utility attention to the security issue is seen in the rapidly growing subscribership of the WaterISAC. This tool provides an invaluable way for utilities, law enforcement, and intelligence analysts to share information in a secure manner. Finally, the AWWA/AMWA survey found that 90 percent of utility respondents report that they have increased or substantially increased their security activities in the past year.

Every indication, then, is that American utilities are responding appropriately and on time to the requirements of the Bioterrorism Act. Having said that, it is also true that continued federal support for the costs of developing vulnerability assessments will be critical to the ability of many medium and smaller utilities to the thorough job required in the time allowed under the law. As noted, vulnerability assessments and emergency response plans can be very expensive, especially when they have to be done quickly.

Vulnerability assessments aren't the only actions water utilities are taking to enhance their security. Utilities are also changing their policies and procedures in ways that will improve security.

Examples include:

- Requiring advance notification of delivery, especially for chemical suppliers, with the driver's name, shipment control number, etc., being matched at the door against the advance notice;
- Developing strict access, parking, and delivery procedures for contractors and providers of services such as landscaping, custodial care, etc.;
- Developing access requirements for cellular phone companies, some of which have installed antennas on elevated storage tanks;
- Coordinating with local law enforcement for increased surveillance and patrolling of utility property;
- Conducting background checks on certain personnel, such as new hires; and
- Developing neighborhood watch groups for critical assets such as tanks and pumping stations located in residential areas.

These policy/procedural changes can have significant impacts in improving overall water facility security.

Obviously utilities don't have the only job to do in protecting America's water supply. Emergency response personnel also have a critical role and are becoming more alert to the water security issue. A number of water systems have conducted "exercises" with local law enforcement and emergency response personnel to simulate steps they would take in a real emergency. Citizens, too, have an important role in water system security. Citizens in many states now know that they should keep a special watch on certain utility property. In a number of cases, citizens have called the utility — or the police — to report suspicious activity around reservoirs, water tanks, or fire hydrants. Such vigilance is invaluable.

Chapter 5— The Challenges Ahead

While the unprecedented partnership between water utilities and USEPA has accomplished a great deal in a relatively short time, and utilities are meeting the deadlines in the Bioterrorism Act, we face many challenges. More funding, research, information sharing, and awareness are critically needed if we are to continually improve the security of the nation's water supply.

Funding

Developing a robust vulnerability assessment requires a significant investment of time and resources. Estimated costs for conducting a large system vulnerability assessment range from approximately $100,000 to several million dollars, depending on the complexity of the system. Additional resources are required to develop or revise the utility's emergency response plan. AWWA has estimated the total national cost to develop vulnerability assessments as required by the Bioterrorism Act to be approximately $500 million.

1. Developing vulnerability assessments is estimated to cost $500 million nationally.

2. Costs of first steps—fences, locks, lights and alarms—will likely exceed $1.6 billion.

3. Congress provided direct grants of up to $115,000.

The national costs of addressing security needs identified in utility vulnerability assessments are not quantified at this time, but they will be large. AWWA has estimated that the costs of the first steps — improved access controls such as fences, locks, perimeter lights, and intruder alarms at critical utility assets — will exceed $1.6 billion. Most large systems serving greater than 100,000 people are just starting to estimate the costs of capital improvements needed to address the findings of their vulnerability assessment. Not surprisingly, there is a large range in the costs of proposed security improvements identified by utilities so far. A small sample of utilities by AWWA revealed security capital costs ranging from $2 to $75 per customer to undertake steps that the utility considered advisable in light of its vulnerability assessment. One utility serving 1.2 million people has estimated that it needs $90 million to enhance the security of its water and wastewater operations. Some utilities may require only modest investment. The large range in these cost estimates is due to substantial differences in the complexity of water systems, but many water systems will be hard pressed to make the significant investments they need to make, and do it quickly, without federal assistance.

In addition to these initial improvements, many utilities are identifying longer-term capital improvements for increased security. For example, a utility might decide to replace all elevated stream crossings or pipes hanging on the side of a bridge with more expensive buried crossings. A utility might build two smaller plants in the future rather than one large plant (a more expensive approach due to dis-economies of scale), in order to provide additional treatment redundancy in the system. A utility might build additional storage tanks, or a larger tank, in the distribution system (over and above what is typically required for operation) in order to have a larger amount of treated water on hand in case of a plant disruption. A utility could decide to have more and larger interconnections with an adjacent water system in order to have more flexibility to "borrow water" in an emergency. The costs of these types of long-term investments for additional redundancy and reliability are difficult to predict, and at this time, they have not been estimated. Again, though, these costs are almost certainly significant.

AWWA has never expected Congress to substantially pay for vulnerability assessments, emergency response plans, or security-related capital improvements, and is dedicated to the proposition that water systems should be self-sustaining through their rates. But federal assistance for the security-related tasks utilities face is important if the job has to be done quickly and thoroughly. Using funds provided in the FY 2002 supplemental appropriation, USEPA provided direct grants of up to $115,000 to help defray the cost of assessments and plans in the largest water systems (those serving 100,000 or more). The need is even more acute in medium-size and smaller systems, where staff are forced to "wear several hats" and where the utility is less likely to have a dedicated security manager. In the AWWA/AMWA survey mentioned earlier, almost one third of respondents reported feeling that they do not currently have adequate technical resources to deal with the terrorist threat. Additional support for utilities to conduct vulnerability assessments and develop emergency response plans should be a federal budget priority.

Training

The tools utilities use to prepare vulnerability assessments and emergency response plans can be complicated. Their use can be time consuming and expensive. They must be used correctly in order to realize their full potential and for utilities to reap their full benefits. To ensure that tools like RAM-W^{SM} are used correctly, utilities, consultants, and others must be trained in their proper use. AWWA is certified to train in the use of RAM-W^{SM} and has made a large commitment to training in its use as well as on other security matters. Even more training is needed. A federal commitment to assist in this training will help ensure that it is available, timely, and affordable to those who need it most.

Research

Research is critically needed to answer a host of important questions. For example, utilities need improved analytical methods that can provide reliable and real-time answers about what might be in the water for a broad range of potential agents that could be used to contaminate it. For some potential agents, existing analytical methods are inaccurate, unreliable, or too slow, which could be a critical matter if emergency room visits are rising rapidly and treatment/response decisions need to be made quickly. Improved analytical methods need to be developed and moved out of research laboratories into the hands of thousands of utilities.

Policy research is also needed. The effectiveness of the first round of security enhancements should be evaluated. Best management practices need to be identified. Security guidelines for new facility design may need to be developed.

USEPA has developed a draft Security Research Action Plan and held a stakeholder meeting in February 2003 this to solicit input on the initial draft. This Action Plan is comprehensive, but priorities need to be set in order for the most critical research to be conducted first. Allocating sufficient funds to complete all of the research detailed in the Security Research Action Plan should be a federal priority as soon as possible.

The AWWA Research Foundation (AwwaRF) is also conducting a substantial amount of security research. AwwaRF, along with USEPA, funded the initial development of RAM-W[SM]. AwwaRF developed an inventory of past security threats and the small system case study for RAM-W[SM]. Ongoing projects include a primer of best management practices to improve security, an analysis of the lessons learned from the first round of vulnerability assessments, and projects to improve analytical methods.

Taken together, security research needs are substantial, and should be a federal budget priority.

Information Sharing

The WaterISAC provides a secure portal for the exchange of sensitive security information. However, a great deal of relevant, even critical, information has been withheld from the WaterISAC. For example, a "State-of-the-Knowledge" (SOK) report was completed in mid-2002 for the White House Office of Homeland Security. This report contains information on a variety of potential contamination agents and the status of analytical methods for those agents. Some of that information is classified. The federal government has offered assurance that summary information would be made available to utilities and that detailed information would be available in an emergency. However, it is not clear how that information will be shared, when it will be shared or who will have access to it. As of now, the SOK report remains unavailable to utilities, researchers, and others who have a legitimate need for access. USEPA has indicated that development of mechanisms for sharing this kind of information appropriately is a high priority. A protocol for sharing this kind of sensitive information with utilities through the WaterISAC should be developed as a national priority as quickly as possible.

Funding is also needed to operate and maintain the WaterISAC. Although USEPA supported its development, the WaterISAC currently operates on subscriber fees. Unlike other critical infrastructure sectors (energy, finance, etc.), the water sector is

predominantly municipal in ownership. Some water utilities may not be able to afford subscriber fees, and aggregate fees may not be high enough to support the WaterISAC at its fullest potential. In that case, important system benefits would be lost. The national interest is served by giving all utilities access to the WaterISAC and by making WaterISAC as robust and utilitarian as possible. Federal support for it is justified and important, at least for the next several years.

Awareness and Vigilance

Utilities are working to instill a strong culture of security throughout every aspect of their operations. Everyone from the guard at the gate, to the receptionist, to the treatment plant operator, to the general manager must be aware that security is an important part of the job. Employees will have to be trained in the use of new analytical methods and new technologies such as intruder alarms and remote cameras. New employees will need to be trained in security as well as in other aspects of their jobs. Call center operators need to be trained on how to obtain the kinds of information the utility needs to make proper decisions quickly.

The general public also needs to be included in this culture of security. As mentioned previously, some utilities have developed a neighborhood watch program for reservoirs, storage tanks, pumping stations, and so forth, located in residential areas. Members of the public can call the utility or local law enforcement if a nonutility vehicle is observed at remote utility locations. The public can be on the lookout for unauthorized use of fire hydrants.

Maintaining this culture of security throughout the utility staff and the general public will be a long-term challenge. Changing the culture can be one of the most difficult things that any organization faces. It is also one of the most effective and least expensive ways we can improve the security of our water supply.

Conclusion

Everyone has a role to play in protecting America's water supply. Utilities have to conduct vulnerability assessments, revise their emergency response plans, make capital investments to install and maintain security improvements where needed, and change their cultures to incorporate security as an important part of the job. Utilities also need to educate the public on what the public can do to help improve security. The public can serve as an extra set of eyes for utilities' facilities. In some cases it may have to accept the need for higher water bills to pay for investments in security.

The federal government also has a critical role in water security. Additional funding is urgently needed. Research, particularly for new and improved analytical methods, needs to be completed and the results shared with utilities as soon as possible. Technical guidance and assistance will be needed for a multitude of security issues.

Finally, the associations that represent and serve water utilities have a role as well. The critical role of AMWA in developing the WaterISAC has been mentioned. AWWA has trained thousands of utility personnel in the development of vulnerability assessments and is revising the RAM-W^{SM} vulnerability assessment method to improve its applicability to medium and smaller water systems. AWWA is also developing programs to train and assist in the revision of emergency response plans. AwwaRF is conducting critical research on security related matters.

The collaboration over the past two years on water security has been unprecedented. While America's water utilities are safe today, they are not immune against a terrorist attack. And a successful attack on the water supply, while unlikely, could be catastrophic. A secure water supply really is a cornerstone of homeland security. With continued teamwork and collaboration, the water community and USEPA can assure that America's water supply remains the safest in the world.

Timeline of Related Events

May 22, 1998 – President Clinton signed Presidential Decision Directive 63 and thereby identified drinking water as one of America's critical infrastructures

September 11, 2001 – Terrorist attacks on New York City and Pentagon

September 11, 2001 – Present– Water utilities increase security in and around their water systems to prevent terrorist attacks

November 2002 – Congress passes Homeland Security Act of 2002, establishing the Department of Homeland Security

June 12, 2002 – President Bush signs into law the Public Health Security and Bioterrorism and Response Act of 2002

June 2002 – AWWA begins conducting training classes on RAM-W^{SM} for developing water system vulnerability assessments

August 1, 2002 – USEPA completes the classified Baseline Threat Report, describing likely modes of terrorist attack and outlining the parameters for vulnerability assessments by community water systems

December 2002 – Water Information Sharing and Analysis Center (WaterISAC) becomes operational

March 31, 2003 – Water systems serving more than 100,000 people submit vulnerability assessments to the USEPA

December 31, 2003 – Water systems serving between 50,000 and 100,000 people are required to submit vulnerability assessments to the USEPA

June 30, 2004 – Water systems serving between 3,300 and 50,000 people are required to submit vulnerability assessments to the USEPA

Advocacy

With its broad base and proven expertise, AWWA is a powerful advocate for meeting public health needs of water quality and supply. AWWA serves as the voice of the drinking water community. AWWA builds bridges with regulators, legislators, special interest groups, and the general public in its stead as a vital resource to its members, the water profession, and the public.

Communications

AWWA is the resource for current and vital information for the water profession. AWWA provides a constant flow of reliable information on technology, trends, and news through its periodicals, Web site, and media outreach. AWWA's published standards, books, manuals, videos, electronic databases, and reports complete the range of communications offered its members.

Conferences

Our members are our greatest resource. That's why AWWA offers numerous, varied opportunities for members to meet, learn, and network at the international, national, and section levels. In addition to comprehensive conferences for water professionals, AWWA hosts a variety of workshops, symposia, teleconferences, and programs focused on specific aspects of water stewardship.

Education and Training

AWWA is the water professional's resource for continuing education and professional development. Materials and instruction are available through a variety of media, from traditional seminars to online courses, teleconferences and webcasts.

Science and Technology

AWWA unites the drinking water community by developing and distributing authoritative scientific and technological knowledge. Through its members, AWWA develops industry standards for products and processes that advance public health and safety. AWWA also provides quality improvement programs for water and wastewater utilities.

Sections

Each AWWA Section is a community. Through involvement in one of AWWA's 43 Sections, water professionals can take advantage of local educational programs, network with peers, influence state or provincial legislation and regulations, and participate in the local and international organization.

For more information contact
Tom Curtis, *AWWA Deputy Executive Director*
202.628.8303
Andrew Hudson, *Senior Public Affairs Manager*
303.734.3410

AWWA is the authoritative resource for knowledge, information, and advocacy to improve the quality and supply of drinking water in North America and beyond. AWWA is the largest organization of water professionals in the world. AWWA advances public health, safety and welfare by uniting the efforts of the full spectrum of the drinking water community. Through our collective strength we become better stewards of water for the greatest good of the people and the environment.

American Water Works Association

6666 West Quincy Avenue
Denver, CO 80235-3098

NON-PROFIT ORG.
U.S. POSTAGE
PAID
DENVER, CO
Permit No. 1180

AWWA is the authoritative resource for knowledge, information, and advocacy to improve the quality and supply of drinking water in North America and beyond. AWWA is the largest organization of water professionals in the world. AWWA advances public health, safety, and welfare by uniting the efforts of the full spectrum of the drinking water community. Through our collective strength we become better stewards of water for the greatest good of the people and the environment.