Order Code RL31294

Safeguarding the Nation's Drinking Water: EPA and Congressional Actions

Updated January 12, 2004

Mary Tiemann
Specialist in Environmental Policy
Resources, Science, and Industry Division

Safeguarding the Nation's Drinking Water: EPA and Congressional Actions

Summary

The events of September 11, 2001, raised new concerns about the security of the nation's drinking water supplies and their vulnerability to attack. Issues include the readiness of water utilities to prevent and respond to attacks on water systems, steps that can be taken to improve preparedness and response capabilities, and the availability of resources to help utilities enhance drinking water security.

After a presidential commission on critical infrastructure protection identified vulnerabilities in the water sector in 1997, the Environmental Protection Agency (EPA), with other federal agencies, water utilities, and state and local governments, began taking steps to improve the security of water systems, although these efforts generally were not targeted to current terrorism concerns. The 1998 Presidential Decision Directive (PDD) 63 on protecting critical infrastructure designated EPA as the lead federal agency for the water sector. However, PDD-63 efforts were focused almost entirely on computer security issues. Since September 2001, EPA and its water sector partners have undertaken a wide range of actions to enhance the security of water supplies and infrastructure from terrorist or other threats.

The 107th Congress, in emergency supplemental appropriations for FY2002 (P.L. 107-117), provided EPA with some $90 million for drinking water security activities. Of this amount, EPA awarded $51 million in grants to large community water systems for performing vulnerability assessments and preparing emergency plans.

The 107th Congress also passed the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (P.L. 107-188), which requires many community water systems to assess their vulnerabilities and prepare emergency preparedness and response plans. The Act authorizes funding for these activities and for emergency grants to states and utilities. It also directs EPA to review methods to prevent, detect, and respond to threats to water safety and infrastructure security.

The Homeland Security Act of 2002 (P.L. 107-296) created a Department of Homeland Security (DHS) and gave DHS responsibility for assessing and protecting the nation's critical infrastructures. The Act did not transfer EPA's water security functions, and in December 2003, the White House issued Homeland Security Presidential Directive/Hspd-7, confirming EPA's lead role in protecting the water infrastructure sector from terrorist attacks or sabotage.

The security status of the nation's water supplies remains on the agenda in the 108th Congress. Oversight issues include the implementation of the drinking water security provisions of the Bioterrorism Act, the availability of funding for utilities to perform vulnerability assessments and make security upgrades, and coordination of EPA and DHS water sector activities. Another issue concerns the status of research and availability of technologies to help utilities identify, remove, and inactivate potential biological and chemical contaminants. This report reviews efforts to increase drinking water security, and will be updated to reflect developments.

Contents

Safeguarding the Nation's Drinking Water: EPA and Congressional Actions

Introduction

Ensuring the security of the nations' drinking water supplies poses a substantial challenge, partly because the number of water systems is very large and also because the responsibility for protecting drinking water safety is shared among federal, state and local governments and utilities. Nationwide, there are approximately 168,000 public water systems, and these systems range greatly in size, serving from as few as 25 persons to more than 1 million persons. Nearly 140,000 of these water systems serve 500 people or fewer. Approximately 360 systems serve more than 100,000 people and provide water to nearly half of the total population served. Because water supplies support many uses (from drinking water to fire suppression), their disruption could have significant impacts.

A 1996 executive order on critical infrastructure protection (E. O. 13010), included water supply systems as one of 8 national infrastructures vital to the security of the United States. In 1997, the President's Commission on Critical Infrastructure Protection (established by the executive order) issued a report on the vulnerabilities of these categories of infrastructures and strategies for protecting them. The Commission identified three attributes crucial to water supply users: water must be available on demand, it must be delivered at sufficient pressure, and it must be safe for use. The Commission concluded that actions affecting any of these factors could be debilitating for the infrastructure.[1]

Major threats to water supplies include: physical destruction of facilities or distribution systems, biological or chemical contamination of supplies, and cyber attacks. The Commission concluded that water supplies had inadequate protection against the threat of chemical or biological contamination, and that technology was insufficient to allow detection, identification, measurement, and treatment of highly toxic, waterborne contaminants. Water utilities were also found to be vulnerable to cyber attacks as they rely increasingly on computers to control water flow and pressure.[2] The Commission determined that information sharing was the most immediate need, and that warning and analytical capabilities and research and development were all insufficient. (For a broader review of water sector security

---

[1] The President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructures. Report of the President's Commission on Critical Infrastructure Protection.* Appendix A, Sector Summary Reports. October 1997. A-45.

[2] Steps taken by some, typically larger, utilities, to avoid Y2K problems enhanced computer system security from certain types of attacks. For more information on cyber security issues, see CRS Report RL31534, *Critical Infrastructure Remote Control Systems and the Terrorist Threat*.

issues (including wastewater facilities and dams), see CRS Report RL32189, *Terrorism and Security Issues Facing the Water Infrastructure Sector*.)

In response to these findings and related developments, President Clinton, in 1998, issued Presidential Decision Directive (PDD) 63 on critical infrastructure protection. Under this directive, a public/private partnership was established to put in place prevention, response, and recovery measures to ensure the security of the nation's critical infrastructures against criminal or terrorist attacks. PDD-63 designated EPA as the lead federal agency for the water supply sector, and EPA appointed the Association of Metropolitan Water Agencies (AMWA) to coordinate the water sector. Before September 11, however, the main focus of PDD-63 efforts for all critical infrastructure sectors was on cyber security. Subsequently, efforts to protect the nation's critical infrastructures have expanded markedly.[3]

EPA Efforts to Protect Drinking Water

EPA believes that the threat of public harm from an attack on the nation's water supplies is small. Nonetheless, in October 2001, the Agency set a goal to ensure that water utilities in all communities (1) have access to scientific information and expertise, (2) assess their vulnerability to a terrorist attack, (3) improve security, and (4) know the immediate steps to take should an attack occur.

For several years, EPA has been working with state, local, and tribal governments, the drinking water industry, training organizations, and other federal agencies to improve preparedness and increase the security of public water supplies. EPA has placed security-related activities into 5 general categories, including: (1) establishing an information center for drinking water alerts or incidents; (2) developing vulnerability assessment tools; (3) identifying actions to minimize vulnerabilities; (4) revising emergency operations plans; and (5) supporting research on biological and chemical contaminants considered to be potential weapons of mass destruction. Several key government and private sector efforts are described below.

Information Sharing. One goal of PDD-63 in 1998 was to establish an Information Sharing and Analysis Center (ISAC) for each critical infrastructure sector. With assistance from EPA and the Federal Bureau of Investigation (FBI), the Association of Metropolitan Water Agencies has led the effort to develop and implement an ISAC for water utilities. The Water ISAC provides a communications link between the water sector and federal homeland security, law enforcement, intelligence, environmental, and public health agencies. It provides a secure, web-based communication system that can be used to: disseminate information regarding threats against the physical and cyber systems of drinking water and wastewater facilities; allow water utilities to share with each other information on security incidents; and provide an opportunity for utilities to have security incidents analyzed by counter-terrorism experts. [4]

---

[3] For more information on PPD-63 and more recent developments, see CRS Report RL30153, *Critical infrastructures: Background, Policy, and Implementation.*

[4] For further information on the Water ISAC, see [http://www.waterisac.org].

Vulnerability Assessment Tools, Training and Technical Assistance. Concern over the security of drinking water infrastructure and supplies had grown among water utilities during the 1990s. In June 2000, the American Water Works Association Research Foundation (AWWARF) and the Sandia National Laboratories, with EPA support, initiated a project to develop a methodology for utilities to use to assess their vulnerabilities and develop plans to minimize identified risks. The original deadline for completing the vulnerability assessment methodology was Spring 2002; however, after the September 11 attacks, the project was expedited and completed in November 2001. This methodology, known as the Risk Assessment Methodology for Water Utilities (RAM-W), is generally considered to be the best tool available for large water systems to use in developing vulnerability assessments.

Subsequently, states and drinking water organizations, in collaboration with EPA, have developed several other vulnerability assessment tools. These tools were developed to assist water systems of various sizes, with a particular focus on the needs of medium and small drinking water systems.

In addition to providing tools, EPA has worked with states and drinking water organizations to provide technical assistance to utilities on a wide range of security matters. Much of this assistance is aimed at helping smaller water systems, which typically are least likely to have the capacity to address security concerns. The Agency has used "train-the-trainer"grants to build a pool of environmental professionals that can provide training and technical assistance to water systems serving fewer than 50,000 people. In addition, on-site assistance for vulnerability assessment and emergency response planning is available to small and medium wastewater utilities at no cost through the Wastewater Operator Training Program.

In April 2002, EPA issued model emergency response guidelines to provide uniform response, recovery and remediation guidance for water utility actions in response in response to man-made or technological emergencies. The guidance describes minimum actions that EPA recommends be carried out by water utilities for various described events, and identifies federal responsibilities and capabilities that can support local response efforts.[5] In July 2002, EPA issued a water security strategy for systems serving fewer than 100,000 persons.[6]

In October 2003, EPA awarded a grant to several associations to support the development of voluntary physical security guidance and standards for water and wastewater systems. The $1.6 million grant supports an initiative developed by the American Society of Civil Engineers, the Water Environment Federation, and AWWA to develop new and update existing industry guidelines and standards to reduce risks associated with terrorist events and natural disasters. The guidance is

---

[5] U.S. Environmental Protection Agency. *Guidance for Water Utility Response, Recovery & Remediation Actions for Man-Made and/or Technological Emergencies*. EPA 810-R-02-001. April 2002. Available at [http://www.epa.gov/safewater/security].

[6] U.S. Environmental Protection Agency. *Water Security Strategy for Systems Serving Populations Less Than 100,000/15 MGD or Less* (for drinking water utilities and for wastewater utilities treating 1,500 million gallons per day (MGD) or less). July 2002. Available at [http://www.epa.gov/safewater/security/index.html].

intended to help local communities mitigate potential risks when constructing new utilities and operating existing ones.

In December 2003, EPA made available the *Response Protocol Toolbox: Planning for and Responding to Contamination Threats to Drinking Water Systems*. This toolbox was developed to help water utilities respond to intentional contamination threats and incidents, and includes separate guides on water utility planning, contamination threat management, site characterization and investigation, and water sample analysis. In 2004, EPA plans to issue two more modules, including a public heath response guide and a remediation and recovery guide.

Funding for Drinking Water Security Activities. In the *Emergency Supplemental Appropriations Act for FY2002* (P.L. 107-117), EPA received roughly $90 million that could be used for drinking water vulnerability assessments. Congress provided another $5 million for state grants for counter-terrorism coordinators to work with EPA and water utilities in assessing drinking water safety.

During FY2002, EPA allocated roughly $89 million of the amount provided in the emergency supplemental appropriation to support security enhancements at the nation's drinking water systems. Of this amount, EPA targeted approximately $80 million to: (1) provide grants to the largest drinking water systems to conduct vulnerability assessments and enhance emergency response plans; (2) provide technical assistance on vulnerability assessments and emergency response plans to small and medium drinking water systems; and (3) refine security-related detection, monitoring, and treatment tools. EPA targeted another $4 million to: accelerate the development and testing of counter-terrorism tools; support training for the development of vulnerability assessments; provide technical assistance; and conduct, test, and implement research on redesign and detection for collection and treatment systems. EPA also used funds to develop tools and provide training for medium and small drinking water systems to assess vulnerabilities and develop emergency response plans. Additionally, EPA allocated $5 million to the states to support homeland security coordination work involving EPA and drinking water utilities.

In FY2002, EPA awarded approximately $51 million in water security grants to 449 large community water systems, which includes all systems that serve more than 100,000 individuals. Grants were made to publicly and privately owned community water systems for as much as $115,000 per grant. EPA allowed utilities to use grant monies to develop vulnerability assessments, emergency response and operating plans, and security enhancement plans and designs. Utilities also could use grant funds for in-house or contractor support; however, funds could not be used for physical improvements.[7]

Although these grants were made only to large systems, EPA has worked with states and utilities to determine the best ways to meet the security needs of small and medium-sized drinking water systems. EPA has provided roughly $17 million of

---

[7] For a list of communities that have received grants, see *Large Drinking Water Utilities Awarded Security Grants* at [http://www.epa.gov/safewater/security/large_grants/list.html], visited January 7, 2004.

FY2002 supplemental funds directly to the states for technical assistance and training for drinking water systems serving fewer than 100,000 people.

For FY2003, EPA requested $16.9 million to assist small and medium-sized systems with vulnerability assessments and emergency response plans, and $5 million in grants to states to support homeland security coordination. The Consolidated Appropriations Resolution for FY2003, H.J.Res. 2 (P.L. 108-7), enacted February 20, 2002, provides this amount. It also contains several drinking water security earmarks, including $2 million for the National Rural Water Association to help small water systems conduct vulnerability assessments. For FY2004, EPA requested roughly $30 million for water security.

In addition to the above resources, EPA has identified numerous security measures that are eligible for funding through the Drinking Water State Revolving Fund (DWSRF) program.[8] Examples of eligible measures include vulnerability assessments, contingency plans, and various facility improvements. Congress has provided approximately $850 million annually for this program in recent years. However, it is uncertain how readily funds might become available for security measures, as the key purpose of the DWSRF is to facilitate compliance with federal drinking water regulations, and competition for these funds can be considerable.

Research. The FY2002 emergency supplemental appropriation provided funds for research and development activities related to homeland security. EPA used some of these resources to evaluate the performance of drinking water treatment systems for their ability to remove and inactivate biological and chemical warfare agents. EPA also supported research projects on other security-related matters, including research on "river spill" and "pipeline" models to determine the fate and transport of contaminants within rivers and streams and within water treatment plants and distribution systems, and research to develop biodetectors for detecting and quantifying biological contaminants in drinking water supplies.

During FY2002, EPA worked with the Department of Defense (DOD), the Centers for Disease Control and Prevention (CDC), the FBI, and the Food and Drug Administration to review, for the Homeland Security Office, what was known about potential biological, chemical, and radiological contaminants; available detection methods; and how to respond to their presence in drinking water.[9] This State-of-the-Knowledge Report was completed in mid-2002. A year later, the American Water Works Association expressed concern that the Administration had not shared with them important information contained in the report; however, the association did note

---

[8] See EPA Fact Sheet, *Use of the Drinking Water State Revolving Fund (DWSRF) to Implement Security Measures at Public Water Systems*. EPA 816-F-02-040. November 2001. Available at [http://www.epa.gov/safewater/dwsrf/security-fs.pdf], visited January 7, 2004.

[9] For a broad discussion of security-related water research issues and needs, see: *H.R. 3178 and the Development of Anti-Terrorism Tools for Water Infrastructure*. Hearing before the Committee on Science, House of Representatives, 107th Congress, 1st session. Serial No. 107-29. 2001. Available at [http://www.house.gov/science].

that EPA had indicated that developing mechanisms for sharing the information, as appropriate, was a high priority.[10]

EPA has been developing a water security research program that builds on information gathered in the interagency state of knowledge assessment. EPA also has been developing a contaminant database listing high risk contaminants and information on the identification, treatment, and potential health effects of such contaminants.

The primary focus of the water security research program is on community water supply, treatment, and distribution infrastructures, and it addresses the research requirements of the Bioterrorism Act. According to EPA's Strategic Plan for Homeland Security, the Agency will work with the Department of Homeland Security, other federal agencies, universities, and the private sector to: (1) review methods to prevent, detect and respond to chemical, biological, and radiological contaminants that could be intentionally introduced in drinking water systems; (2) review methods and means by which terrorists could disrupt the supply of safe drinking water; and (3) review methods and means by which alternative supplies of drinking water could be provided in the event of a disruption.[11]

EPA's FY2004 budget request proposed a rigorous and specific agenda for drinking water security research for FY2004, with efforts focused in several areas. Key research topics and related activities include:

- *contaminant detection and characterization* (testing and verifying devices to detect contaminants, characterizing contaminants that pose threats, developing standard field screening and laboratory analysis methodologies);

- *contaminant containment* (developing methods and procedures to prevent the spread of contaminants in drinking water sources);

- *drinking water decontamination* (developing technologies and procedures to decontaminate water, including developing point-of-use and point-of-entry technologies for removing contaminants and new methods to neutralize, analyze, and remediate contamination);

- *scientific and technical support* (including developing a database of contaminant characteristics for first responders, refining detection, containment, and decontamination technologies based on vulnerability assessments, improving coordination of water managers and public health officials, and enhancing physical security of water systems); and

---

[10] American Water Works Association. *Protecting Our Water: Drinking Water Security in America After 9/11*. Journal of the American Water Works Association. July 2003. p. 45.

[11] U.S. Environmental Protection Agency. *Strategic Plan for Homeland Security. September 2002.* p. 4. This report and more information on EPA's water security activities and plans are available online at: http://www.epa.gov/safewater.

- *risk communication* (instituting monitoring approaches and networks to help public health officials identify and control disease outbreaks, and transferring techniques and technologies to utility managers and first responders).[12]

National Strategy for the Physical Protection of Critical Infrastructure and Key Assets

In February 2003, the White House issued the *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* which spells out national policy and guiding principles for key infrastructure sectors. Consistent with PDD-63, this strategy designated EPA as the lead federal agency charged with coordinating critical water infrastructure protection activities and developing cooperative relationships with its sector counterparts (i.e., state and local governments and water utilities).

The strategy noted that the water sector "has taken great strides to protect its critical facilities and systems."[13] It further stated that the water sector was focusing on four categories of possible attacks that could have the greatest human health or economic consequences. These areas include: (1) physical damage or destruction of critical assets (including the intentional release of toxic chemicals); (2) actual or threatened contamination of the water supply; (3) cyber attack; and (4) interruption of services from another infrastructure (such as energy supply[14]).

To address these potential threats, the strategy cautioned that the water sector requires better threat information to focus investments on security measures. It further cautioned that the sector required increased monitoring and analytic capabilities to enhance detection of biological, chemical, or radiological contaminants that could be intentionally introduced into the water supply. It specifically identified the need for new analytical methods, monitoring strategies, sampling protocols and training, and noted that additional resources would likely be needed.

To address gaps in water infrastructure protection efforts, the strategy presented four initiatives and outlined the respective roles of EPA and DHS:

- EPA is directed to work with DHS, state and local governments, and other water sector leaders to identify methods to better secure key points of storage and distribution (e.g., dams, pumping stations, chemical storage facilities and treatment plants). EPA and DHS will

---

[12] U.S. Environmental Protection Agency. *FY2004 Annual Performance Plan and Congressional Justification.* p. II-15 - II-16.

[13] Office of Homeland Security. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. February 2003. p. 39

[14] For example, the electrical blackout that occurred in August 2003 caused numerous problems at drinking water and wastewater systems in New York and Michigan. Power failures at drinking water plants required utilities to issue boil water advisories in numerous communities. This blackout heightened questions regarding the preparedness of the nation's public water systems to respond to emergency situations, including terrorist incidents.

continue providing tools, training, technical assistance and some financial assistance for research on vulnerability assessment methodologies and risk management strategies;

- EPA will continue leading efforts to improve information on contaminants of concern and to develop monitoring and analytical capabilities.

- DHS and EPA will continue working to improve sector-wide information exchange and coordinate contingency planning; and

- DHS and EPA will work with other sectors to manage risks resulting from sector interdependencies. EPA will convene working groups to develop models for integrating priorities and emergency response plans.

While this strategy provides guiding principles for the critical infrastructure sectors, particular agency actions are likely to become clearer as the Administration articulates specific implementation procedures and details. The strategy's stated goals, identified gaps, and related resource needs may generate congressional attention in several venues, including oversight and appropriations.

Congressional Actions to Enhance Drinking Water Security

The 107th Congress held multiple hearings to examine security issues facing the water infrastructure sector[15] and acted on several bills to improve drinking water security. The bills ranged from requiring utilities to assess and reduce vulnerabilities, to providing assistance to utilities for security enhancements, to establishing research programs to improve utilities' ability to prevent, mitigate, and respond to attacks. Enacted bills are discussed below.

The *Emergency Supplemental Appropriations Act for FY2002* (P.L. 107-117), enacted in January 2002, provided EPA with $175.6 million for emergency expenses to respond to the September 11 attacks and to support counter-terrorism activities. The accompanying conference report, H.Rept. 107-350, specified that roughly $90 million was intended to be used to improve security at EPA laboratories, to perform drinking water vulnerability assessments, and for anthrax decontamination activities. Another $5 million was for state grants for counter-terrorism coordinators to work with EPA and water utilities in assessing drinking water safety.

Bioterrorism Preparedness Act. In June 2002, the President signed into law the *Public Health Security and Bioterrorism Preparedness and Response Act of 2002* (P.L. 107-188, H.Rept. 107-481). The House-passed version of the bill

---

[15] See, for example, *Terrorism: Are Our Water Resources and Environment at Risk?* Hearing before the Subcommittee on Water Resources and Environment of the Committee on Transportation and Infrastructure, House of Representatives. 107th Congress, 1st session. (107-51) October 10, 2001. 147 p.

contained drinking water security provisions, and the final act expanded on these provisions, including elements of Senate water security bills.

Title IV of the Bioterrorism Act (42 U.S.C. 300i) amended the Safe Drinking Water Act (SDWA) to requires each community water system serving more than 3,300 individuals to conduct an assessment of the system's vulnerability to terrorist attacks or other intentional acts to disrupt the provision of a safe and reliable drinking water supply. These systems must certify to EPA that they have conducted a vulnerability assessment and submit a copy of the assessment to EPA. The Act also requires these systems to prepare or revise emergency response plans incorporating the results of the vulnerability assessments no later than 6 months after completing them. Table 1 outlines the schedule for water utilities to submit vulnerability assessments to EPA and to complete emergency response plans.[16]

Table 1. Community Water System Requirements under the Bioterrorism Act

System size by population served (est. no. of systems)	Vulnerability assessments must be completed	Emergency response plans must be completed
100,000 or more (425)	March 31, 2003	September 30, 2003
50,000 - 99,999 (460)	December 31, 2003	June 30, 2004
3,301 - 49,999 (7,500)	June 30, 2004	December 31, 2004

The Act exempts the contents of the vulnerability assessments from disclosure under the Freedom of Information Act (except for information contained in the certification identifying the system and the date of the certification). The law directed EPA to develop protocols to protect the assessments from unauthorized disclosure, and provides for civil and criminal penalties for inappropriate disclosure of information by government officials.

Additionally, the Bioterrorism Preparedness Act requires each community water system serving more than 3,300 individuals to prepare or revise an emergency response plan incorporating the results of the vulnerability assessment no later than 6 months after completing the assessment. EPA was required to provide guidance to smaller systems on how to conduct vulnerability assessments, prepare emergency response plans, and address threats.[17]

---

[16] In January 2003, EPA issued *Instructions to Assist Community Water Systems in Complying with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002*. Office of Water. EPA 810-B-02-110. Available at Internet Web site: [http://www.epa.gov/safewater/security/community.html], visited January 7, 2004.

[17] In July, 2002, EPA published *Water Security Strategy for Systems Serving Populations Less than 100,000/15MGD or Less*. Available at Internet Web site:

(continued...)

The Bioterrorism Act authorized $160 million for FY2002, and such sums as may be necessary for FY2003-FY2005, to provide financial assistance to community water systems to conduct vulnerability assessments, to prepare response plans, and for expenses and contracts to address basic security enhancements and significant threats. (Security enhancements may include purchase and installation of intruder detection equipment and lighting, enhancing security of automated systems, personnel training and security screening of employees or contractors, etc. Funding may not be used for personnel costs, plant operations, monitoring or maintenance.)

For EPA to make grants to states and water systems to assist in responding to emergency situations, the Act authorized $35 million for FY2002, and such sums as may be necessary thereafter. Finally, the Act authorized $15 million for FY2002, and such sums as may be necessary for FY2003 through FY2005, for EPA to review methods by which terrorists or others could disrupt the provision of safe water supplies, and methods for preventing, detecting, and responding to such disruptions.

Homeland Security Act of 2002. In November 2002, President Bush signed into law the *Homeland Security Act of 2002* (P.L. 107-296) which combined the functions of all or parts of 22 federal agencies and departments into a new Department of Homeland Security (DHS).[18] The Act gave key responsibility for critical infrastructure protection to DHS, but did not transfer EPA water security functions to the new Department.

The Homeland Security Act established within DHS a Directorate for Information Analysis and Infrastructure Protection, headed by an undersecretary. The responsibilities of the undersecretary include:

- receiving, analyzing, and integrating law enforcement, intelligence and other information to identify and assess the nature and scope of terrorist threats to the United States;
- assessing vulnerabilities of key resources and critical infrastructure; integrating information, analyses, and vulnerability assessments to identify priorities for protective and support measures;
- ensuring timely access by DHS to all necessary information; and
- developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States.[19]

---

[17] (...continued)
[http://www.epa.gov/safewater/security/med-small-strategy.pdf], visited January 7, 2004.

[18] For more information, see CRS Report RL31493, *Homeland Security: Department Organization and Management - Legislative Phase*, and CRS Report RL31751 *Homeland Security: Department Organization and Management - Implementation Phase*.

[19] See also CRS Report RL30153, *Critical Infrastructures: Background, Policy, and Implementation*.

Under the Bioterrorism Act, Congress gave EPA new authorities and responsibilities to assist water utilities and states in enhancing the security of drinking water supplies and facilities, and directed water utilities to assess vulnerabilities and to submit their vulnerability assessments to EPA. Also, the *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* designated EPA as the lead agency for protecting critical water infrastructure, consistent with PDD-63. With the creation of DHS, which has overall responsibility for critical infrastructure vulnerability assessment and protection, it was unclear what the relationship would be between EPA and the Department.

In December 2003, the White House issued Homeland Security Presidential Directive/Hspd-7, which supersedes PDD-63. This Directive establishes national policy and outlines the roles and responsibilities of federal departments and agencies regarding critical infrastructure protection. It identifies EPA as the federal agency with lead responsibilities for ensuring the protection of the water infrastructure sector from terrorist attacks or sabotage. The Directive gives DHS responsibility for overall coordination and integration of national critical infrastructure protection efforts by federal, state, and local governments and the private sector.

Issues in the 108th Congress

With the continuing concern over the potential for terrorist attacks, Congress has remained concerned about the security status of the nation's public water supplies and infrastructure. Interest in the 108th Congress generally has focused on funding for, and implementation of, the drinking water security provisions of the Bioterrorism Act, and on other efforts to enhance the security and emergency preparedness of public water systems. Because of actions on the part of the drinking water community, EPA, and Congress, efforts to enhance security in the drinking water sector appear to be ahead of those in certain other sectors (for example, chemical facilities). However, a number of issues and challenges remain.

A key issue concerns the availability of funding and technical resources for communities to perform vulnerability assessments and, subsequently, to make the necessary security upgrades. The AWWA estimates that the total national cost for community water systems to develop vulnerability assessments, as required by the Bioterrorism Act, to be roughly $500 million. Estimates of costs for a large system to conduct a vulnerability assessment range from $100,000 to several million dollars, depending on the system's complexity.[20] Notably, this estimate does not include the cost of making security upgrades to address vulnerabilities identified in the assessments; Congress has not provided funding specifically for this purpose.

Small water systems, which are not required to prepare vulnerability assessments and response plans, also face security challenges. Although these systems encounter lower security costs than large systems, they generally are the least likely to have the technical and financial resources to address security concerns. Consequently, they may be perceived to be more vulnerable than large systems. In the absence of any

---

[20] American Water Works Association. *Protecting Our Water: Drinking Water Security in America After 9/11*. Journal of the American Water Works Association. July 2003. p. 43.

direct federal financial assistance, EPA, states, and water associations have been providing guidance and technical assistance for medium and small systems.

The Consolidated Appropriations Resolution for FY2003, P.L. 108-7 (H.J. Res. 2), provided EPA with the amount the Administration requested for drinking water security activities: $16.9 million to assist small and medium-sized systems with vulnerability assessments and emergency response plans, and $5 million in grants to states to support homeland security coordination. It also contains several drinking water security earmarks, including $2 million for the National Rural Water Association to help small water systems conduct vulnerability assessments.

Another policy issue involves the uncertainty about the quality of efforts to improve security taken by the drinking water sector. In 2002, EPA stated that, as utilities that are required to assess vulnerabilities and develop emergency response plans complete their work, EPA and states will evaluate whether appropriate security measures have been implemented.[21] The results of these evaluations may be another issue of oversight interest to the Congress. Such oversight efforts could be complicated by the Bioterrorism Act's requirement that EPA develop protocols to protect vulnerability assessments from disclosure to unauthorized individuals. This issue could become of added interest, should Congress decide to make funding available for security upgrades. According to a recent General Accounting Office (GAO) report, security experts generally agree that decisions for allocating federal funding for security improvements should be based primarily on two criteria: (1) population density, and (2) information from vulnerability assessments.[22]

A major concern for the water sector is the need for more research to develop real-time monitoring methods to detect contaminants, and technologies to remove or inactivate them. The GAO survey of security experts found strongest support for research on developing monitoring technologies that can quickly detect contaminants in water that has already left a treatment plant for distribution to consumers.[23] The EPA Office of Research and Development's National Homeland Security Research Center (NHSRC) and Office of Water's Water Security Division are developing the Water Security Research Action Plan to define a program of research and technical support for protecting water systems from terrorist attacks. EPA also has been working on a contaminant database listing high risk contaminants and information on the identification, treatment, and potential health effects of such contaminants. Progress in these efforts also may be an issue of oversight interest.

---

[21] U.S. Environmental Protection Agency. *Strategic Plan for Homeland Security*. p. 5.

[22] U.S. General Accounting Office. *Drinking Water: Experts' Views on How Future Federal Funding Can Best Be Spent to Improve Security*. Report to the Committee on Environment and Public Works, U.S. Senate. October 2003. GAO-04-29. p. 6.

[23] Ibid. p. 7.