Order Code RL31294

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

Updated March 7, 2003

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 raised 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 concerns over terrorism. Pursuant to the 1998 Presidential Decision Directive (PDD) 63 on protecting critical infrastructure, EPA provided some assistance to improve preparedness and increase the security of water systems. However, PDD-63 efforts were focused almost entirely on computer security issues. Since September 11, 2001, EPA has increased efforts to help utilities safeguard facilities and supplies from terrorist or other threats in numerous ways (e.g., by providing technical and financial assistance for vulnerability assessments and by supporting research and the establishment of an information sharing center).

The 107th Congress took significant steps to improve drinking water security. In the emergency supplemental appropriations for FY2002 (P.L. 107-117), Congress provided EPA with roughly $90 million for drinking water security. Of this amount, EPA awarded $51 million in grants to large community water systems to assess their vulnerability to terrorist attacks and to prepare emergency response plans.

The 107th Congress also passed the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (P.L. 107-188, H.Rept. 107-481), which requires many community water systems to perform vulnerability assessments and to prepare emergency preparedness and response plans. The legislation authorizes funding for systems to carry out these activities and for emergency assistance grants to states and public water systems. 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) established a Department of Homeland Security and gave it responsibility for evaluating the vulnerabilities of critical infrastructures. The Act did not transfer EPA's water security activities and responsibilities. In February 2003, the White House issued the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, which designates EPA as the lead agency for protecting critical water infrastructure.

The 108th Congress may be interested in overseeing implementation of the water security provisions of the Bioterrorism Act and other efforts to improve drinking water security. Regarding funding, the Consolidated Appropriations Resolution for FY2003, P.L. 108-7 (H.J.Res. 2) provides more than $22 million for EPA for water security activities. This report 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. Another 360 systems serve more than 100,000 people and provide water to nearly half of the total population served. Because water supplies directly affect many activities (from drinking water to fighting fires), 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 identified in the report 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 water utilities, typically larger utilities, to avoid Y2K problems have enhanced computer system security from certain types of attacks. For more information on this security issue, see CRS Report RL31534, *Critical Infrastructure Remote Control Systems and the Terrorist Threat*.

issues (including wastewater facilities and dams), see CRS Report RS21026, *Terrorism and Security Issues Facing the Water Infrastructure Sector*.)

In response to these findings and other developments, President Clinton issued Presidential Decision Directive (PDD) 63 on critical infrastructure protection in 1998.[3] 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 focus of the PDD-63 efforts for all critical infrastructure sectors was on cyber security. Subsequently, efforts to protect the nation's critical infrastructures have been broadened and accelerated.[4]

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, the Agency has 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.[5]

For several years, but most substantially since September 11, 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 water supplies. Security-related activities fall into 5 general categories including: developing vulnerability assessment tools, identifying actions to minimize vulnerabilities, revising and enhancing existing emergency operations plans, establishing an information center on drinking water alerts or incidents, and 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, within 5 years, 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 a secure ISAC for water utilities. The Water ISAC provides a Web-based communication system that can be used to (1) disseminate early warnings and alerts regarding threats against the physical and cyber systems of drinking water and wastewater facilities; (2) allow water utilities to share with each other information on security incidents; and (3) provide an opportunity for utilities

---

[3] See [http://www.ciao.gov/resource/directive.html].

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

[5] U.S. Environmental Protection Agency. *EPA Actions to Safeguard the Nation's Drinking Water Supplies.* October 2001. See [http://www.epa.gov/safewater/security/index.html].

to have security incidents analyzed by counter-terrorism experts. It was officially launched in December 2002 and will become fully operational during FY2003.[6]

Among other initiatives to provide information to utilities, notices were distributed to utilities and local law enforcement officials on measures they could take immediately to improve security. Also, EPA sent several notices to utilities outlining available resources and providing advice on monitoring and treatment.

Vulnerability Assessment Training and Technical Assistance. Among water utilities, concerns over the security of facilities and supplies had been increasing in recent years. In response to these concerns, the American Water Works Association Research Foundation (AWWARF) initiated a project in June 2000 with the Department of Energy's Sandia National Laboratories to develop a vulnerability assessment methodology for utilities to use to assess vulnerabilities and develop plans to minimize identified risks. The original deadline for completing the vulnerability assessment methodology was Spring 2002; however, after the attacks of September 11, the project was expedited and completed in November 2001.

With EPA support, the American Water Works Association (AWWA) has offered workshops and training for water utilities on a wide range of security topics, including risk and vulnerability assessment, emergency response planning, and risk communication. This training has included workshops based on the vulnerability assessment methodology developed by Sandia National Laboratories which has enabled a number of large water utilities to acquire tools to evaluate their security and improve the preparedness of their water systems against intentional acts or emergency events.[7] Funds provided in the FY2002 emergency supplemental appropriations (P.L. 107-117) allowed EPA to provide vulnerability assessment training to many other utilities during 2002. Training initially has been directed to community water systems that serve 100,000 or more people.

EPA also has worked with states, tribes, and utility organizations to provide technical assistance to utilities on security matters. In April 2002, EPA issued model emergency response guidelines to provide uniform response, recovery and remediation guidance for water utility actions in response to man-made or technological emergencies. In addition to describing minimum actions that EPA recommends be carried out by water utilities for various described events, the guidance document also identifies federal responsibilities and capabilities that can support local response efforts.[8] In July 2002, EPA issued a water security strategy for systems serving fewer than 100,000 persons.[9] In June, the Association of State

---

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

[7] For more information, see the American Water Works Association Research Foundation Web site at [http://www.awwarf.com/press/security.pdf].

[8] 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].

[9] U.S. Environmental Protection Agency. *Water Security Strategy for Systems Serving* (continued...)

Drinking Water Administrators and the National Rural Water Association, in collaboration with EPA, published a security vulnerability self-assessment guide for small drinking water systems (serving fewer than 3,300 people). A similar guide was issued in November 2002 for systems serving population between 3,300 and 10,000.

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.

By the end of FY2002, EPA had awarded more than $51 million in water security grants to 449 large community water systems (i.e., systems serving more than 100,000 individuals). EPA has made grants for vulnerability assessments and other security planning to publicly and privately owned community water systems for as much as $115,000 per grant. According to EPA,

> grant monies may be used to develop a vulnerability assessment, emergency response/operating plan, security enhancement plans and designs, or a combination of the efforts. Utilities may use grant funds for in-house or contractor support, assuming demonstration of qualifications. ... Funds awarded under this program may not be used for physical improvements.[10]

Although these grants have been 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

---

[9] (...continued)
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). Available at [http://www.epa.gov/safewater/security/index.html].

[10] 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].

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 has 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.[11] Examples of eligible measures include vulnerability assessments, contingency plans, and various facility improvements. Congress approved $850 million for this program for each of FY2002 and FY2003. 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 because it can take years for a public water system to receive funding through this infrastructure program.[12]

Research. The FY2002 emergency supplemental appropriation provided funds for research and development activities related to homeland security. EPA has 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. Additionally, EPA has supported research projects on other security-related matters. Projects have included 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.[13]

---

[11] For more information, 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].

[12] Another potential source of funding for community water systems to enhance security may be through the U.S. Department of Agriculture, Rural Utility Service (RUS), Water and Environmental Programs. These programs provide grants, loans, and loan guarantees for water and waste disposal projects for communities of 10,000 or fewer individuals. According to RUS officials, funds provided for community water system projects could be used to improve the security of those systems. For FY2002, the RUS had available for the Water and Environmental Programs approximately $586 million for grants, $836 million in direct loan authority, and $75 million in guaranteed loan authority. For FY2003, RUS received $723 million for these programs. In addition, Congress provided in the 2002 Farm Bill (P.L. 107-171) $360 million to fund water and waste disposal applications that were pending on the date of Farm Bill's enactment, May 13, 2002. This is mandatory funding that does not require an appropriation.

[13] Statement of Marianne Horinko, Assistant Administrator, Office of Solid Waste and Emergency Response, U.S. Environmental Protection Agency, before the Subcommittee on

(continued...)

Relatedly, 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 develop information for the Homeland Security Office on biological, chemical, and radiological contaminants, and how to respond to their presence in drinking water. This effort was intended to expand the state of knowledge on: technologies to detect contaminants, monitoring protocols and techniques, and treatment effectiveness.[14]

In support of the President's National Strategy for Homeland Security, EPA issued the Agency's *Strategic Plan for Homeland Security* in September 2002. Regarding drinking water research, the plan generally incorporates the research requirements of the Bioterrorism Preparedness Act (outlined below). Specifically, the plan states that EPA 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. (The full text of this Agency-wide strategic plan is available at [http://www.epa.gov/epahome/headline_100202.htm].

EPA's FY2004 budget request proposes a rigorous agenda for drinking water security research for FY2004, with efforts focused in several areas. Key research areas include: 1) contaminant detection (testing and verifying devices to detect contaminants, characterizing contaminants that pose threats, developing standard field screening and laboratory analysis methodologies); 2) contaminant containment (developing methods and procedures to prevent the spread of contaminants in drinking water sources); 3) 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); 4) 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 5) 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).[15]

---

[13] (...continued)
Water Resources and Environment of the Committee on Transportation and Infrastructure. October 10, 2001.

[14] 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].

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

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 designates 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 notes that the water sector "has taken great strides to protect its critical facilities and systems."[16] It further states that, in order to set priorities within the range of protection measures that could be taken, the water sector is focusing on four categories of possible attacks that could have the greatest human health or economic consequences. These areas of concentration 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).

To address these potential threats, the strategy cautions that the water sector requires better threat information to focus investments on security measures. It further cautions that the sector requires 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 identifies the need for new analytical methods, monitoring strategies, sampling protocols, and training and notes that additional resources are likely to be needed.

Beyond current efforts to protect water infrastructure, the strategy identifies additional efforts that are needed to address threats. The following four initiatives are presented:

- EPA, working with DHS, state and local governments, and other water sector leaders, will work 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 also 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

---

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

- 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, its functions are likely to become clearer as the Administration articulates specific implementation procedures and details. The strategy's goals and related potential 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[17] 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, H.R. 3338), enacted January 10, 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 contained drinking water security provisions, and the final act expanded on these provisions, including elements of other Senate bills on water security.

Title IV of the Bioterrorism Act amended the Safe Drinking Water Act (SDWA) to require 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. The law establishes deadlines, based on system size, for these systems to certify to EPA that they have conducted a vulnerability assessment and to submit to EPA a copy of the assessment. Deadlines for certifications and submissions are as follows:

---

[17] 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.

- March 31, 2003, for systems serving 100,000 or more persons;
- December 31, 2003, for systems serving 50,000 or more but fewer than 100,000 persons; and
- June 30, 2004, for systems serving more than 3,300 but fewer than 50,000 persons.[18]

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.[19]

Congress 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.[20]

Department of Homeland Security. The Department of Homeland Security proposal announced by the Administration in June 2002 envisioned a Department

---

[18] 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].

[19] In July, 2002, EPA published *Water Security Strategy for Systems Serving Populations Less than 100,000/15MGD or Less*. Available at Internet Web site: [http://www.epa.gov/safewater/security/med-small-strategy.pdf].

[20] For a detailed discussion of the entire Act and a chronology of bioterrorism hearings, see CRS Report RL31263, *Bioterrorism: Legislation to Improve Public Health Preparedness and Response Capacity.*

that, among other things, would be responsible for "comprehensively evaluating the vulnerabilities of America's critical infrastructure," including water systems. The proposal discussed a national effort to secure critical infrastructure sectors by building and maintaining a comprehensive assessment of these sectors. As proposed, the Department would analyze threats, direct or coordinate action to protect vulnerable systems, and "establish policy for standardized, tiered protective measures tailored to the target and rapidly adjusted to the threat."

After months of congressional deliberations and various modifications to the original proposal, President Bush signed into law the *Homeland Security Act of 2002* (P.L. 107-296, H.R. 5005) on November 25, 2002.(For further discussion, see CRS Report RL31493, *Homeland Security: Department Organization and Management*.)

The Homeland Security Act does not transfer EPA water security functions to the new Department of Homeland Security, and does not specifically mention water infrastructure. The Act states that "critical infrastructure" has the meaning given the term in section 1016(e) of the Patriot Act (P.L. 107-56), i.e.,

> systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

The Act establishes within DHS a Directorate for Information Analysis and Infrastructure Protection to be headed by an undersecretary, and to include an Assistant Secretary for Information Analysis and an Assistant Secretary for Infrastructure Protection.[21] 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.

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. Consequently, it was not clear how

---

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

these activities might be affected by the Homeland Security Act, which gives overall responsibility for critical infrastructure vulnerability assessment to DHS.

As noted above, the *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*, issued by the White House in February 2002, designates EPA as the lead agency for protecting critical water infrastructure. This is consistent with PDD-63, which designated EPA as the lead agency for the water sector in 1998. Specific procedures to facilitate information sharing and other collaboration between EPA and DHS are still being developed.

Actions in the 108th Congress. With the continuing concern over the potential for terrorist attacks, as reflected in the ongoing elevated threat advisory level designated by DHS, Congress remains interested in the security status of the Nation's water supplies and resources. Among other actions, the 108th Congress may be interested in overseeing the implementation of the drinking water security provisions of the Bioterrorism Act as well as other efforts to enhance the security and emergency preparedness of drinking water systems, including the initiatives outlined in the national critical infrastructure protection strategy.

Congressional attention could focus on a range of questions, including: 1) what are the roles of EPA and states in overseeing implementation of the Bioterrorism Act security requirements by drinking water utilities; 2) what are the relative roles and responsibilities of EPA and DHS regarding water infrastructure protection, including efforts related to vulnerability assessments and information sharing; and 3) what additional funding may be needed by public water systems to meet the new mandates or to make security improvements, and from what source(s) might such funding come? Another issue concerns what additional efforts and funding may be required at the federal and state levels to address the water sector threats identified in the national critical infrastructure protection strategy (e.g., the need for better monitoring and analytical capabilities and improved information exchange and contingency planning).

Regarding funding, the Consolidated Appropriations Resolution for FY2003, P.L. 108-7 (H.J.Res. 2), provides 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.