Order Code RL32189

CRS Report for Congress
Received through the CRS Web

Terrorism and Security Issues Facing the Water Infrastructure Sector

Updated March 15, 2004

Claudia Copeland
Specialist in Resources and Environmental Policy
Resources, Science, and Industry Division

Betsy Cody
Specialist in Natural Resources Policy
Resources, Science, and Industry Division

Terrorism and Security Issues Facing the Water Infrastructure Sector

Summary

Damage to or destruction of the nation's water supply and water quality infrastructure by terrorist attack could disrupt the delivery of vital human services in this country, threatening public health and the environment, or possibly causing loss of life. Interest in such problems has increased greatly since the September 11, 2001, terrorist attacks in New York City and at the Pentagon.

Across the country, water infrastructure systems extend over vast areas, and ownership and operation responsibility are both public and private but are overwhelmingly non-federal. Since the attacks, federal dam operators and water and wastewater utilities have been under heightened security conditions and are evaluating security plans and measures. There are no federal standards or agreed-upon industry best practices within the water infrastructure sector to govern readiness, response to security incidents, and recovery. Efforts to develop protocols and tools are ongoing since the 2001 terrorist attacks. This report presents an overview of this large and diverse sector, describes security-related actions by the government and private sector since September 11, and discusses additional policy issues and responses, including congressional interest.

Policymakers are considering a number of initiatives, including enhanced physical security, better communication and coordination, and research. A key issue is how additional protections and resources directed at public and private sector priorities will be funded. In response, Congress has provided $483 million in appropriations for security at water infrastructure facilities (to assess and protect federal facilities and support vulnerability assessments by non-federal facilities) for FY2002, FY2003 and FY2004, and passed a bill requiring drinking water utilities to conduct security vulnerability assessments (P.L. 107-188). Congress also gave the newly created Department of Homeland Security responsibilities to coordinate information to secure the nation's critical infrastructure, including the water sector (P.L. 107-297). Continuing attention to these issues in the 108th Congress is anticipated. Current interest is focusing on bills concerning security of wastewater utilities (H.R. 866, S. 1039). This report will be updated as warranted.

Contents

Terrorism and Security Issues Facing the Water Infrastructure Sector

Introduction

The September 11, 2001, attacks on the World Trade Center and the Pentagon have drawn attention to the security of many institutions, facilities, and systems in the United States, including the nation's water supply and water quality infrastructure.[1] These systems have long been recognized as being potentially vulnerable to terrorist attacks of various types, including physical disruption, bioterrorism/chemical contamination, and cyber attack. Damage or destruction by terrorist attack could disrupt the delivery of vital human services in this country, threatening public health and the environment, or possibly causing loss of life. This report presents an overview of this large and diverse sector, describes security-related actions by the government and private sector since September 11, and discusses additional policy issues and responses, including congressional interest.

The potential for terrorism is not new. In 1941, Federal Bureau of Investigation Director J. Edgar Hoover wrote, "It has long been recognized that among public utilities, water supply facilities offer a particularly vulnerable point of attack to the foreign agent, due to the strategic position they occupy in keeping the wheels of industry turning and in preserving the health and morale of the American populace."[2] Water infrastructure systems also are highly linked with other infrastructures, especially electric power and transportation, as well as the chemical industry which supplies treatment chemicals, making security of all of them an issue of concern. These types of vulnerable interconnections were evident, for example, during the August 2003 electricity blackout in the Northeast United States: wastewater treatment plants in Cleveland, Detroit, New York, and other locations that lacked backup generation systems lost power and discharged millions of gallons of untreated sewage during the emergency, and power failures at drinking water plants led to boil-water advisories in many communities.

Background

Broadly speaking, water infrastructure systems include surface and ground water sources of untreated water for municipal, industrial, agricultural, and household needs; dams, reservoirs, aqueducts, and pipes that contain and transport raw water;

---

[1]For additional information, see the CRS Electronic Briefing Book on Terrorism [http://www.congress.gov/brbk/html/ebter1.html].

[2] Hoover, J.E. "Water Supply Facilities and National Defense." *Journal of the American Water Works Association*. Vol. 33, no. 11 (1941): 1861.

treatment facilities that remove contaminants from raw water; finished water reservoirs; systems that distribute water to users; and wastewater collection and treatment facilities. Across the country, these systems comprise more than 75,000 dams and reservoirs; thousands of miles of pipes, aqueducts, water distribution, and sewer lines; 168,000 public drinking water facilities (many serving as few as 25 customers); and about 16,000 publicly owned wastewater treatment facilities. Ownership and management are both public and private; the federal government has ownership responsibility for hundreds of dams and diversion structures, but the vast majority of the nation's water infrastructure is either privately owned or owned by non-federal units of government.

The federal government has built hundreds of water projects, primarily dams and reservoirs for irrigation development and flood control, with municipal and industrial water use (M&I) as an incidental, self-financed, project purpose. Many of these facilities are critically entwined with the nation's overall water supply, transportation, and electricity infrastructure. The largest federal facilities were built and are managed by the Bureau of Reclamation (Bureau) of the Department of the Interior and the U.S. Army Corps of Engineers (Corps) of the Department of Defense.

Bureau reservoirs, particularly those along the Colorado River, supply water to millions of people in southern California, Arizona, and Nevada via Bureau and non-Bureau aqueducts. Bureau projects also supply water to 9 million acres of farmland and other municipal and industrial water users in the 17 western states. The Corps operates 276 navigation locks, 11,000 miles of commercial navigation channel, and approximately 1,200 projects of varying types, including 609 dams. It supplies water to thousands of cities, towns, and industries from the 9.5 million acre-feet of water stored in its 116 lakes and reservoirs throughout the country, including service to approximately one million residents of the District of Columbia and portions of northern Virginia. The largest Corps and Bureau facilities also produce enormous amounts of power. For example, Hoover and Glen Canyon dams on the Colorado River represent 23% of the installed electrical capacity of the Bureau of Reclamation's 58 power plants in the West and 7% of the total installed capacity in the Western United States. Similarly, Corps facilities and the Bureau's Grand Coulee Dam on the Columbia River provide 43% of the total installed hydroelectric capacity in the West (25% nationwide).

A fairly small number of large drinking water and wastewater utilities located primarily in urban areas (about 15% of the systems) provide water services to more than 75% of the U.S. population. Arguably, these systems represent the greatest targets of opportunity for terrorist attacks, while the large number of small systems that each serve fewer than 10,000 persons are less likely to be perceived as key targets by terrorists who might seek to disrupt water infrastructure systems. However, the more numerous smaller systems also tend to be less protected and, thus, are potentially more vulnerable to attack, whether by vandals or terrorists. A successful attack on even a small system could cause widespread panic, economic impacts, and a loss of public confidence in water supply systems.

Attacks resulting in physical destruction to any of these systems could include disruption of operating or distribution system components, power or

telecommunications systems, electronic control systems, and actual damage to reservoirs and pumping stations. A loss of flow and pressure would cause problems for customers and would hinder firefighting efforts. Further, destruction of a large dam could result in catastrophic flooding and loss of life. Bioterrorism or chemical attacks could deliver widespread contamination with small amounts of microbiological agents or toxic chemicals, and could endanger the public health of thousands. While some experts believe that risks to water systems actually are small, because it would be difficult to introduce sufficient quantities of agents to cause widespread harm, concern and heightened awareness of potential problems are apparent. Factors that are relevant to a biological agent's potential as a weapon include its stability in a drinking water system, virulence, culturability in the quantity required, and resistance to detection and treatment. Cyber attacks on computer operations can affect an entire infrastructure network, and hacking in water utility systems could result in theft or corruption of information or denial and disruption of service.

Responses to Security Concerns

Federal dam operators went on "high-alert" immediately following the September 11 terrorist attacks. The Bureau closed its visitor facilities at Grand Coulee, Hoover, and Glen Canyon dams. Because of potential loss of life and property downstream if breached, security threats are under constant review, and coordination efforts with both the National Guard and local law enforcement officials are ongoing. The Corps also operates under continued high defense alert and temporarily closed all its facilities to visitors after September 11, although locks and dams remained operational; most closed facilities later re-opened, but security is being reassessed. Following a heightened alert issued by the federal government in February 2003, the Bureau implemented additional security measures which remain in effect at dams, powerplants, and other facilities, including limited access to facilities and roads, closure of visitor centers, and random vehicle inspections.

Although officials believe that risks to water and wastewater utilities are small, operators have been under heightened security conditions since September 11. Local utilities have primary responsibility to assess their vulnerabilities and prioritize them for necessary security improvements. Most (especially in urban areas) have emergency preparedness plans that address issues such as redundancy of operations, public notification, and coordination with law enforcement and emergency response officials. However, many plans were developed to respond to natural disasters, domestic threats such as vandalism, and, in some cases, cyber attacks. Drinking water and wastewater utilities coordinated efforts to prepare for possible Y2K impacts on their computer systems, but these efforts focused more on cyber security than physical terrorism concerns. Thus, it was unclear whether previously existing plans incorporate sufficient procedures to address other types of terrorist threats. Utility officials are reluctant to disclose details of their systems or these confidential plans, since doing so might alert terrorists to vulnerabilities.

Water supply was one of eight critical infrastructure systems identified in President Clinton's 1998 Presidential Decision Directive 63 (PDD-63)[3] as part of a coordinated national effort to achieve the capability to protect the nation's critical infrastructure from intentional acts that would diminish them. These efforts focused primarily on the 340 large community water supply systems which each serve more than 100,000 persons. The Environmental Protection Agency (EPA) was identified as the lead federal agency for liaison with the water supply sector. In response, in 2000, EPA established a partnership with the American Metropolitan Water Association (AMWA) and American Water Works Association (AWWA) to jointly undertake measures to safeguard water supplies from terrorist acts. AWWA's Research Foundation has contracted with the Department of Energy's Sandia National Laboratory to develop a vulnerability assessment tool for water systems (as an extension of methodology for assessing federal dams). EPA is supporting an ongoing project with the Sandia Lab to pilot test the physical vulnerability assessment tool and develop a cyber vulnerability assessment tool. An Information Sharing and Analysis Center (ISAC) supported by an EPA grant became operational under AMWA's leadership in December 2002. It will allow for dissemination of alerts to drinking water and wastewater utilities about potential threats or vulnerabilities to the integrity of their operations that have been detected and viable resolutions to problems.[4]

Some research on water sector infrastructure protection is underway. The Department of the Army is conducting research in the area of detection and treatment to remove various chemical agents. The Federal Emergency Management Agency (FEMA) is leading an effort to produce databases of water distribution systems and to develop assessment tools for evaluating threats posed by the introduction of a biological or chemical agent into a water system. The Centers for Disease Control and Prevention is developing guidance on potential biological agents and the effects of standard water treatment practices on their persistence. However, in the January 2001 report of the President's Commission on Critical Infrastructure Protection, ongoing water sector research was characterized as a small effort that leaves a number of gaps and shortfalls relative to U.S. water supplies.[5] This report stated that gaps exist in four major areas, concerns that remain relevant and are guiding policymakers now.

- Threat/vulnerability risk assessments,
- Identification and characterization of biological and chemical agents,
- A need to establish a center of excellence to support communities in conducting vulnerability and risk assessment, and

---

[3]"The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63." [http://www.fas.org/irp/offdocs/paper598.htm], visited March 15, 2004.

[4]For additional information, see: [http://www.waterisac.org/aboutisac.asp], visited January 5, 2004.

[5] Critical Infrastructure Assurance Office. *Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities*. January 2001. [http://www.fas.org/irp/offdocs/pdd/CIP_2001_CongRept.pdf], visited March 15, 2004.

- Application of information assurance techniques to computerized systems used by water utilities, as well as the oil, gas, and electric sectors, for operational data and control operations.

Less attention has been focused on protecting wastewater treatment facilities than drinking water systems, perhaps because destruction of them probably represents more of an environmental threat (i.e., by release of untreated sewage) than a direct threat to life or public welfare. Vulnerabilities do exist, however. Large underground collector sewers could be accessed by terrorist groups for purposes of placing destructive devices beneath buildings or city streets. Damage to a wastewater facility prevents water from being treated and can impact downriver water intakes. Destruction of containers that hold large amounts of chemicals at treatment plants could result in release of toxic chemical agents, such as chlorine gas, which can be deadly to humans if inhaled and, at lower doses, can burn eyes and skin and inflame the lungs. Since the terrorist attacks, many utilities have switched from using chlorine gas as disinfection to alternatives which are believed to be safer, such as sodium hypochlorite or ultraviolet light. However, some consumer groups remain concerned that many wastewater utilities continue to use chlorine gas, including facilities that serve heavily populated areas. To prepare for potential accidental releases of hazardous chemicals from their facilities, 3,460 wastewater and drinking water utilities already are subject to risk management planning requirements under the Clean Air Act, but some observers advocate requiring federal standards to ensure that facilities using dangerous chemicals, such as wastewater treatment plants, use the best possible industry practices to reduce hazards.[6]

There are no federal standards or agreed-upon industry best practices within the water infrastructure sector to govern readiness, response to security incidents, and recovery. Efforts to develop protocols and tools are ongoing since the 2001 terrorist attacks. Wastewater and drinking water utility organizations are implementing computer software and training materials to evaluate vulnerabilities at large, medium, and small utility systems, and EPA has provided some grant assistance for conducting vulnerability assessments. Out of funds appropriated in January 2002 (P.L. 107-117), EPA awarded $51 million for vulnerability assessment grants to 449 large drinking water utilities, averaging $115,000 per utility. Out of subsequent appropriations, EPA has been targeting grants to "train the trainers," delivering technical assistance to organizations such as the Rural Community Assistance Program and the Water Environment Federation that, in turn, can assist and train personnel at thousands of medium and small utilities throughout the country. With financial support from EPA, water and engineering groups are developing voluntary physical security standards for drinking water and wastewater systems that could serve as a model for future EPA voluntary standards; EPA is not currently authorized to require water infrastructure systems to undertake specific security measures or meet particular security standards.

---

[6] See, for example, Environmental Defense. *Eliminating Hometown Hazards, Cutting Chemical Risks at Wastewater Treatment Facilities.* December 2003. 14 p. [http://www.environmentaldefense.org/documents/3357_EliminatingHometownHazards.pdf], visited January 5, 2004.

EPA has taken a number of organizational and planning steps to strengthen water security. The agency created a National Homeland Security Research Center within the Office of Research and Development to develop the scientific foundations and tools that can be used to respond to attacks on water systems. In September 2003, it created a Water Security Division, taking over activities initiated by a Water Protection Task Force after the September 11 terrorist attacks. The office will train water utility personnel on security issues, support the WaterISAC, and implement the agency's comprehensive research plan. EPA has issued both a Water Security Research and Technical Support Action Plan, identifying critical research needs and providing an implementation plan for addressing those needs, and a Strategic Plan for Homeland Security.[7] The Strategic Plan, which is not limited to water security concerns, identifies four mission-critical areas on which EPA intends to focus its homeland security planning: critical infrastructure protection; preparedness, response, and recovery; communication and information; and protection of EPA personnel and information.

There has been criticism of some of these EPA efforts, however. A preliminary review of the Research and Action Plan by a panel of the National Research Council identified some gaps, suggested alternative priorities, and noted that the Plan is silent on the financial resources required to complete the research and to implement needed countermeasures to improve water security.[8] EPA's Inspector General recently issued an evaluation report on the Strategic Plan for Homeland Security and concluded that the agency has not outlined how resources, activities, and outputs will achieve the water security program's goals. Moreover, the Inspector General said that EPA lacks fundamental components, such as performance measures, for monitoring program performance against goals.[9] EPA responded that long-term objectives for critical water infrastructure protection activities may be identified in a future revised strategic plan.

Federal officials have been reassessing federal infrastructure vulnerabilities for several years. The Bureau of Reclamation's site security program is aimed at ensuring protection of the Bureau's 252 high- and significant-hazard dams and facilities and 58 hydroelectric plants. After September 11, the Bureau committed to conducting vulnerability and risk assessments at 280 high-priority facilities. Risk assessments were completed at 156 of these in FY2002 and FY2003; the remaining facilities are to be completed in FY2004. These assessments resulted in

---

[7] U.S. Environmental Protection Agency. *Strategic Plan for Homeland Security*. September 2002. 62 p. [http://www.epa.gov/epahome/downloads/epa_homeland_security_strategic_plan.pdf], visited January 5, 2004.

[8] National Academies Press. *A Review of the EPA Water Security Research and Technical Support Action Plan: Parts I and II*. Water Science and Technology Board. 2003. [http://www.nap.edu/books/0309089824/html], visited January 5, 2004.

[9] U.S. Environmental Protection Agency. Office of Inspector General. *EPA Needs a Better Strategy to Measure Changes in the Security of the Nation's Water Infrastructure*. Report No. 2003-M-00016, Sept. 11, 2003. [http://www.epa.gov/oig/reports/2003/HomelandSecurityReport2003M00016.pdf], visited January 5, 2004.

recommendations now being implemented to enhance security procedures and physical facilities, such as additional security staffing, limited vehicle and visitor access, and coordination with local law enforcement agencies. The Corps implements a facility protection program to detect, protect, and respond to threats to Corps facilities and a dam security program to coordinate security systems for Corps infrastructure. It also implements a national emergency preparedness program which assists civilian governments in responding to all regional/national emergencies, including acts of terrorism. Both agencies participate in the Interagency Committee on Dam Safety (ICODS), which is part of the National Dam Safety Program that is led by FEMA.

A February 2003 White House report[10] presented a national strategy for protecting the nation's critical infrastructures and identified four water sector initiatives: identify high-priority vulnerabilities and improve site security; improve monitoring and analytic capabilities; improve information exchange and coordinate contingency planning; and work with other sectors to manage unique risks resulting from interdependencies. It also proposed establishing an ISAC for information sharing among dam operators. The strategy is intended to focus national protection priorities, inform resource allocation processes, and be the basis for cooperative public and private protection actions.

Department of Homeland Security. The newly created Department of Homeland Security (DHS, established in P.L. 107-297[11]) has a mandate to coordinate securing the nation's critical infrastructure, including water infrastructure, through partnerships with the public and private sectors. It is responsible for detailed implementation of core elements of the national strategy for protection of critical infrastructures. One of its tasks is to assess infrastructure vulnerabilities, an activity that wastewater and drinking water utilities have been doing since September 11, under their own initiatives and congressional mandates (P.L. 107-188, discussed below). The legislative reorganization did not transfer Corps or Bureau responsibilities for security protection of dams and other facilities or EPA's responsibilities to assist drinking water and wastewater utilities.

In December 2003, President Bush issued Homeland Security Presidential Directive/Hspd-7 which establishes a national policy for the federal government to identify, prioritize, and protect critical infrastructure as a part of homeland security.[12] The directive calls for DHS to integrate all security efforts among federal agencies and to complete a comprehensive national plan for critical infrastructure protection by December 2004. The document supersedes PDD-63, which started the process

---

[10] The White House. Office of Homeland Security. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.* 90 p. [http://www.whitehouse.gov/homeland/book/index.html], visited January 5, 2004.

[11] For current information on the Department, see CRS products identified at: [http://www.congress.gov/erp/legissues/html/isdhs2.html].

[12] The White House. *December 17, 2003 Homeland Security Presidential Directive/Hspd-7, Critical Infrastructure Identification, Prioritization, and Protection.* [http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html], visited January 5, 2004.

of federal protection of critical infrastructure even before the 2001 terrorist attacks. Under Hspd-7, EPA continues as the lead federal agency to ensure protecting drinking water and wastewater treatment systems from possible terrorist acts and other sabotage.

Appropriations. In P.L. 107-38, the 2001 Emergency Supplemental Appropriations Act, enacted one week after September 11, Congress appropriated $40 billion for recovery from and response to the terrorist attacks. The President allocated $20 billion of this total (about $30 million went to water infrastructure), and in October 2001, he requested allocation of the remaining $20 billion to be distributed by Congress. The request included $245 million for federal water infrastructure programs: $30 million for security at Bureau facilities; $139 million for security at Corps facilities; and $45.5 million to EPA for drinking water vulnerability assessments. P.L. 107-117, the DOD and Emergency Supplemental Appropriations Act for FY2002, provided the full amounts requested for the Bureau and the Corps and increased funding for EPA, including $91 million to strengthen security at large drinking water systems through vulnerability assessments and other non-structural security efforts.

In July 2002, Congress approved an FY2002 supplemental appropriations bill that included $50 million more in EPA grants for vulnerability assessments by small and medium-size drinking water systems and $108 million for security activities at Corps facilities (P.L. 107-206). However, on August 13, President Bush announced that he would not spend $5.1 billion of contingent emergency funds in the bill, including the EPA grant and Corps funds. (For information, see CRS Report RL31406, *Supplemental Appropriations for FY2002: Combating Terrorism and Other Issues*.)

The President's FY2003 budget requested $115 million for security at water infrastructure facilities, consisting of $28.4 million for the Bureau; $65 million for the Corps; and $22 million for EPA, including $15 million for vulnerability assessments at small and medium-size drinking water systems. Final action on appropriations for these agencies was delayed until February 2003. In P.L. 108-7, Congress appropriated $85 million for water infrastructure security programs, approving the amounts requested for EPA and the Bureau, but $30 million less than was requested for the Corps' facility security program. In P.L. 108-11, the FY2003 supplemental appropriations bill, Congress provided an additional $39 million for the Corps and $25 million for the Bureau, for increased security measures at their facilities.

For FY2004, Congress appropriated funds for water infrastructure security at levels requested by the Administration, including $32.2 million for EPA to support utility vulnerability assessments and the WaterISAC (in P.L. 108-199), $12.9 million for the Corps, and $27.8 million for the Bureau (appropriations for the Bureau and

the Corps are included in P.L. 108-137).[13] Appropriations for water infrastructure security have totaled $482.8 million since the September 11 attacks.

The President's FY2005 budget requests $66.3 million for water security, consisting of:

- $11.1 million for EPA (to support training and development of voluntary industry best practices for security; the request is $21 million less than the FY2004 request, largely due to the completion of vulnerability assessments by drinking water utilities, which EPA has previously assisted);
- $43.2 million for the Bureau ($15.4 million more than was requested for FY2004), intended to fund full implementation of the agency's physical security, personnel and information security, and law enforcement program and to advance the physical hardening improvements that were identified in the Bureau's security risk assessments in FY2002; and
- $12 million for the Corps (approximately the same as requested for FY2004) to cover non-project specific protective measures at Corps administrative buildings and other general use facilities. Also, the Corps budget requests an additional $72 million for security measures at various specific individual water resource projects around the country.

Policy Issues and Congressional Responses

Congress and other policymakers are considering a number of initiatives in this area, including enhanced physical security, communication and coordination, and research. Regarding physical security, a key question is whether protective measures should be focused on the largest water systems and facilities, where risks to the public are greatest, or on all, since small facilities may be more vulnerable. A related question is responsibility for additional steps, because the federal government has direct control over only a limited portion of the water infrastructure sector. The adequacy of physical and operational security safeguards is an issue for all in this sector. One possible option for federal facilities (dams and reservoirs maintained by the Bureau and the Corps) is to restrict visitor access, including at adjacent recreational facilities, although such actions could raise objections from the public. Some operators of non-federal facilities and utilities are likewise concerned. As a precaution after September 11, New York City, which provides water to 9 million consumers, closed its reservoirs indefinitely to all fishing, hiking, and boating and blocked access to some roads.

Policymakers also are examining measures that could improve coordination and exchange of information on vulnerabilities, risks, threats, and responses. This is a key objective of the WaterISAC and also of the Department of Homeland Security, which includes, for example, functions of the National Infrastructure Protection

---

[13] FY2004 appropriated amounts reflect a provision in P.L. 108-199 which mandated a 0.59% rescission to accounts and to each nondefense discretionary program, project and activity funded by that legislation, as well as previously enacted FY2004 appropriations acts, including P.L. 108-137.

Center (NIPC) of the FBI that brings together the private sector and government agencies at all levels to protect critical infrastructure, especially on cyber issues. One issue of interest is how the new Department is coordinating its activities with ongoing security efforts by other federal agencies and non-federal entities that operate water infrastructure systems, including its implementation of the comprehensive national plan required by the recent Presidential Directive/Hspd-7. This issue has arisen in recent weeks as a result of moves by DHS to assert authority over water utility security, despite claims by EPA that it is the lead federal agency. For example, DHS is preparing guidance documents on how each infrastructure sector, including water systems, can protect itself from security threats, and DHS contractors have visited several water utilities and asked to view pertinent information, including the utilities' vulnerability assessments. EPA sources have said that the DHS contractors may not have authority to view the vulnerability assessments, but Department officials have reportedly cited Hspd-7 as giving the department authority to conduct water system inspections, because of its lead role in coordinating critical infrastructure protection. Since February, the two agencies have been working to clarify their roles in providing security to water utilities.

One particular communication/coordination issue concerns the extent of EPA's ability to collect and analyze security data from water utilities, especially information in vulnerability assessments submitted under the Bioterrorism Preparedness Act (discussed below). EPA officials believe that the Act permits reviewing utility submissions for overall compliance and allows aggregation of data but precludes the agency from asking for or analyzing data showing changes in security levels, as a safeguard against unintended release of such information. Others, including EPA's Inspector General, believe that EPA has the authority and responsibility to review and analyze the information in order to identify and prioritize threats and to develop plans to protect drinking water supplies.

Among the research needs being addressed are tools for vulnerability and risk analysis, identification and response to biological/chemical agents, real-time monitoring of water supplies, and development of information technology. The cost of additional protections and how to pay for them are issues of interest, and policymakers continue to consider resource needs and how to direct them at public and private sector priorities. An issue of increasing interest to drinking water and wastewater utilities is how to pay for physical security improvements, since currently there are no federal funds dedicated to these purposes.

The 107th and 108th Congresses have conducted oversight on a number of these issues and considered legislation to address various policy issues, including government reorganization, and additional appropriations. In May 2002, Congress approved the Public Health Security and Bioterrorism Preparedness and Response Act (P.L. 107-288). Title IV of that act requires drinking water systems serving more than 3,300 persons to conduct vulnerability analyses and to submit the assessments to EPA. The legislation authorizes grant funding to assist utilities in meeting these requirements. (For information, see CRS Report RL31294, *Safeguarding the Nation's Drinking Water: EPA and Congressional Actions.)* Legislation authorizing the Bureau to contract with local law enforcement to protect its facilities also was enacted during the 107th Congress (P.L. 107-69).

In 2001, the House and Senate considered but did not enact legislation authorizing a 6-year grant program for research and development on security of water supply and wastewater treatment systems (H.R. 3178, S. 1593). Some of the drinking water research provisions in these bills were included in the Bioterrorism Preparedness Act. In October 2002, the House approved a bill authorizing $220 million in grants and other assistance for vulnerability assessments by wastewater treatment utilities (H.R. 5169), but the Senate did not act on a related bill (S. 3037). In the 108th Congress, legislation authorizing vulnerability assessment grants to wastewater utilities (H.R. 866, identical to H.R. 5169 in the 107th Congress) was approved by the House on May 7, 2003, by a 413-7 vote. The Senate Environment and Public Works Committee approved related legislation on May 15 (S. 1039, S.Rept. 108-149). No further action has occurred, due in part to concerns expressed by some that the legislation does not require that vulnerability assessments be submitted to EPA, as is the case with drinking water assessments required by the 2002 Bioterrorism Preparedness Act. Continuing attention to these issues is anticipated during the 108th Congress.