Order Code RL32189

CRS Report for Congress

Terrorism and Security Issues Facing the Water Infrastructure Sector

Updated November 16, 2007

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

Prepared for Members and
Committees of Congress

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 the United States.

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 have been 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 $789 million in appropriations for security at water infrastructure facilities (to assess and protect federal facilities and support vulnerability assessments by non-federal facilities) and passed a bill requiring drinking water utilities to conduct security vulnerability assessments (P.L. 107-188). When Congress created the Department of Homeland Security (DHS) in 2002 (P.L. 107-297), it gave DHS responsibilities to coordinate information to secure the nation's critical infrastructure, including the water sector. Under Homeland Security Presidential Directive-7, the Environmental Protection Agency (EPA) is the lead federal agency for protecting drinking water and wastewater utility systems.

Recent congressional interest has focused on bills concerning security of wastewater utilities. In the 109th Congress, the Senate Environment and Public Works Committee approved legislation to encourage wastewater treatment works to conduct vulnerability assessments and develop site security plans (S. 2781), but there was no further action on this bill. Similar legislation has been introduced in the 110th Congress (S. 1968). Continuing attention to these issues is possible, along with interest in how the federal government coordinates its own activities and communicates policies and information to the water infrastructure sector.

Contents

List of Figures

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. 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. Further, since most water infrastructure is government-owned, it may serve as a symbolic and political target for some. 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."[1] Water infrastructure systems also are highly linked with other infrastructure systems, 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; treatment facilities that remove contaminants from raw water; finished water

---

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

reservoirs; systems that distribute water to users; and wastewater collection and treatment facilities. Across the country, these systems comprise approximately 77,000 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 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). Still, despite its critical involvement in such projects, especially in the West, the federal government is responsible for only about 5% of the dams whose failure could result in loss of life or significant property damage. The remaining dams belong to state or local governments, utilities, and corporate or private owners.

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

Water infrastructure system designers, managers, and operators have long made preparing for extreme events a standard practice. Historically, their focus has been on natural events — major storms, blizzards, and earthquakes — some of which could be predicted hours or longer before they occurred. When considering the risk of manmade threats, operators generally focused on purposeful acts such as vandalism or theft by disgruntled employees or customers, rather than broader malevolent threats by terrorists, domestic or foreign. The events of September 11, 2001, changed this focus.

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 some 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 on January 1, 2000, 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)[2] 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.[3]

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.[4] This report stated that gaps exist in four major areas, concerns that remain relevant and are guiding policymakers now.

---

[2] "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63," May 22, 1998; see [http://www.fas.org/irp/offdocs/paper598.htm].

[3] For additional information, see [http://www.waterisac.org/].

[4] Critical Infrastructure Assurance Office, *Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities,* January 2001, 209 p. See [http://www.iwar.org.uk/cip/resources/ciao/final-ciao.pdf].

- 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
- 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 likely 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. Pipelines can be made into weapons via the introduction of a highly flammable substance such as gasoline through a manhole or inlet. Explosions in the sewers can cause collapse of roads, sidewalks, and adjacent structures and injure and kill people nearby. 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 water and wastewater 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, 2,816 wastewater and drinking water utilities, water supply systems, and irrigation systems 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 (practices that are referred to as Inherently Safer Technologies, or ISTs) to reduce hazards.[5]

In March 2006, the Government Accountability Office (GAO) reported on a survey of security measures at 200 of the nation's largest wastewater utilities.[6] GAO found that many have made security improvements since the 2001 terrorist attacks. Most utilities said they have completed, or intend to complete, a plan to conduct some type of security assessment. More than half of responding facilities indicated

---

[5] See, for example, Environmental Defense, *Eliminating Hometown Hazards, Cutting Chemical Risks at Wastewater Treatment Facilities*, December 2003, 14 p. Center for American Progress, *Toxic Trains and the Terrorist Threat, How Water Utilities Can Get Chlorine Gas Off the Rails and Out of American Communities*, April 2007, 23 p.

[6] U.S. Government Accountability Office, *Securing Wastewater Facilities, Utilities Have Made Important Upgrades but Further Improvements to Key System Components May Be Limited by Costs and Other Constraints*, GAO-06-390, March 2006, 64 p.

they did not use potentially dangerous gaseous chlorine as a wastewater disinfectant. However, the report noted that these utilities have made little effort to address collection system vulnerabilities, due to the technical complexity and expense of securing collection systems that cover large areas and have many access points. Some told GAO investigators that taking other measures, such as converting from gaseous chlorine, took priority over collection system protections. In a 2007 follow-on study, GAO reported that actual and projected capital costs to convert from chlorine gas to alternative disinfection methods range from about $650,000 to just over $13 million. Factors affecting conversion costs included the type of alternative method; the size of the facility; and labor, building, and supply costs, which varied considerably.[7]

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. EPA is not authorized to require water infrastructure systems to implement specific security improvements or meet particular security standards. Efforts to develop voluntary 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 to drinking water utilities for 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, drinking water and wastewater utility, and engineering groups have developed three security guidance documents, issued in December 2004, that cover the design of online contaminant monitoring systems, and physical security enhancements of drinking water, wastewater, and stormwater infrastructure systems. The documents provide voluntary guidelines for assisting utilities that have completed vulnerability assessments to mitigate vulnerabilities of their systems through the design, construction, operation, and maintenance of both new and existing systems. Based on the three guidance documents, these groups also have drafted training materials and a set of voluntary standardized best engineering practices that recommend measures to protect water and wastewater infrastructure against a range of threats, including terrorist attacks and other sources of potential harm, such as accidents, chemical contamination, and natural disasters.[8]

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

---

[7] U.S. Government Accountability Office, *Securing Wastewater Facilities, Costs of Vulnerability Assessments, Risk Management Plans, and Alternative Disinfection Methods Vary Widely*, GAO-07-480, March 2007, 26 p.

[8] See [http://www.asce.org/static/1/wise.cfm].

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 trains water utility personnel on security issues, supports the WaterISAC, and implements the agency's comprehensive research plan. Early in 2004, EPA formed an advisory group of drinking water and wastewater utilities, called the Water Security Working Group, to advise on the development of best security practices and policies for water utilities.

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. The Strategic Plan, which is not limited to water security concerns, identifies several mission-critical areas on which EPA intends to focus its homeland security planning: critical infrastructure protection; preparedness, response, and recovery; communication and information; protection of EPA personnel and infrastructure; and self-evaluation.

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.[9] In 2003, EPA's Inspector General issued an evaluation report on the initial Strategic Plan for Homeland Security and concluded that the agency had 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.[10] EPA responded that long-term objectives for critical water infrastructure protection activities could be identified in a future revised strategic plan. A second Homeland Security Strategy, issued in October 2004, updates the initial strategy principally by reflecting projected funding and resources for the next two years on EPA's strategic objectives and recognizing the evolving role of the Department of Homeland Security.[11]

GAO has issued two reports discussing how future federal funding can best be spent to improve security at drinking water and wastewater utilities.[12] Both reports are based on the views of subject matter experts identified by GAO. In the drinking water report, specific activities judged by the experts to be most deserving of federal

---

[9] 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.

[10] 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, September 11, 2003.

[11] U.S. Environmental Protection Agency, "Homeland Security Strategy," October 2004, 46 p.

[12] U.S. Government Accountability Office, *Drinking Water, Experts' Views on How Future Federal Funding Can Best Be Spent to Improve Security*, GAO-04-29, October 2003, 69 p. U.S. Government Accountability Office, *Wastewater Facilities, Experts' Views on How Federal Funds Should Be Spent to Improve Security*, GAO-05-165, January 2005, 70 p.

support included physical and technological upgrades, education and training for staff and responders, and strengthening key relationships between water utilities and others such as law enforcement and public health agencies. In the wastewater report, the experts cited the replacement of gaseous chemicals used in the disinfection process with less hazardous alternatives as a key activity deserving of federal funds, along with improving local, state, and regional collaboration, and support facilities' vulnerability assessments. Asked how federal funds should be allocated, both groups of experts favored giving priority to utilities that serve critical assets (such as public health institutions, government, and military bases) and to utilities serving areas with large populations.

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 at these facilities were completed between FY2002 and FY2004. These assessments resulted in 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[13] 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. 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 Department of Homeland Security (DHS, established in P.L. 107-297) 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 the September 11 attacks, under their own initiatives and congressional mandates (P.L. 107-288; see page 13). The legislative reorganization did not transfer Corps or Bureau

---

[13] The White House, Office of Homeland Security, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, February 2003, 90 p.

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.[14] The directive called 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 Department missed that deadline for completing a National Infrastructure Protection Plan. A February 2005 interim report focusing on federal role and outlining a risk management framework to guide future efforts was criticized for the fact that it failed to address private sector roles — an important element, since nearly 85% of the nation's infrastructure is in private hands. In 2006, DHS issued a National Infrastructure Protection Plan (NIPP) that is intended to set national priorities, goals, and requirements for effective distribution of funding and resources to help ensure that government, the economy, and public services continue in the event of a terrorist attack or other disaster. It proposes a framework of partnerships between private industry sectors and the government that would work together to secure the nation's vital resources. For example, EPA would work with water treatment and wastewater systems, while dams would cooperate with DHS. In response to the NIPP, those agencies, in conjunction with private industry partners, state and local governments, and utility agencies, prepared 17 sector-specific plans which were completed in May 2007. The plans identify sector profiles and assets, assess risks, prioritize infrastructure, identify sector protection plans and measures of progress. The water sector plan for wastewater and drinking water focuses on four goals: (1) sustaining protection of public health and the environment; (2) recognize and reduce risks; (3) maintain a resilient infrastructure; and (4) increase communication, outreach, and public confidence.[15] The sector plan for dams, including federal dams, is one of 10 that DHS determined presents security sensitivity issues if widely distributed; thus, those 10 plans were not released to the public.

In the NIPP, DHS described a plan to develop a risk analysis method that would include a uniform means of measuring risk and assessing consequences across infrastructure sectors. Some drinking water and wastewater treatment industry officials commented that this plan, known as the Risk Analysis and Management for Critical Asset Protection (RAMCAP), raised concern that it could force some facilities to conduct new, or revise existing, vulnerability assessments. Drinking water industry officials are said to be concerned that a new method may not recognize vulnerability assessments that many drinking water utilities have already

---

[14] The White House, *December 17, 2003 Homeland Security Presidential Directive/ HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection.* HSPD-7 superseded PDD-63, which started the process of federal protection of critical infrastructure even before the 2001 terrorist attacks.

[15] U.S. Department of Homeland Security and U.S. Environmental Protection Agency, *Water, Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan*, May 2007, 122 p.
See [http://www.dhs.gov/xlibrary/assets/Water_SSP_5_21_07.pdf].

completed under requirements of the 2002 Bioterrorism Preparedness Act (see page 13).

Coordination and Information Sharing. The Homeland Security Department's involvement in water security concerns has been growing, although under HSPD-7, EPA continues as the lead federal agency to ensure protection of drinking water and wastewater treatment systems from possible terrorist acts and other sabotage. Since early 2004 DHS has been preparing guidance documents on how each infrastructure sector, including water systems, can protect itself from security threats. DHS contractors 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 cited HSPD-7 as giving the department authority to conduct water system inspections, because of its lead role in coordinating critical infrastructure protection. For some time, the two agencies have been working to clarify their roles in providing security to water utilities.

In the fall of 2004, water utilities formed a new 24-member group, the Water Sector Coordinating Council, to work with federal officials. For example, this Council collaborated on the sector-specific plan for water that was completed in May 2007. One of its functions is to be a point of contact for DHS to vet potential water security policies, allowing one-stop shopping for federal officials. Also at that time, DHS created a new information-sharing network, called the Homeland Security Information Network (HSIN). Both it and the existing WaterISAC share the goal of providing security information to water utilities, but they differ in some respects. The WaterISAC is a private, subscription service (although it receives some federal funding) that provides information to about 530 water utilities and others on security matters. The HSIN, a software program, is a free, federally funded platform for information sharing. It is not limited to the water sector, and it provides no information by itself; it acts as a bulletin board where DHS, EPA, and utilities can post security-related information. Distinct from the HSIN and the WaterISAC is the Water Security Channel (WaterSC), launched in 2004 as a free service of the WaterISAC, which disseminates EPA and DHS general security bulletins at the request of those agencies to more than 8,000 utilities.

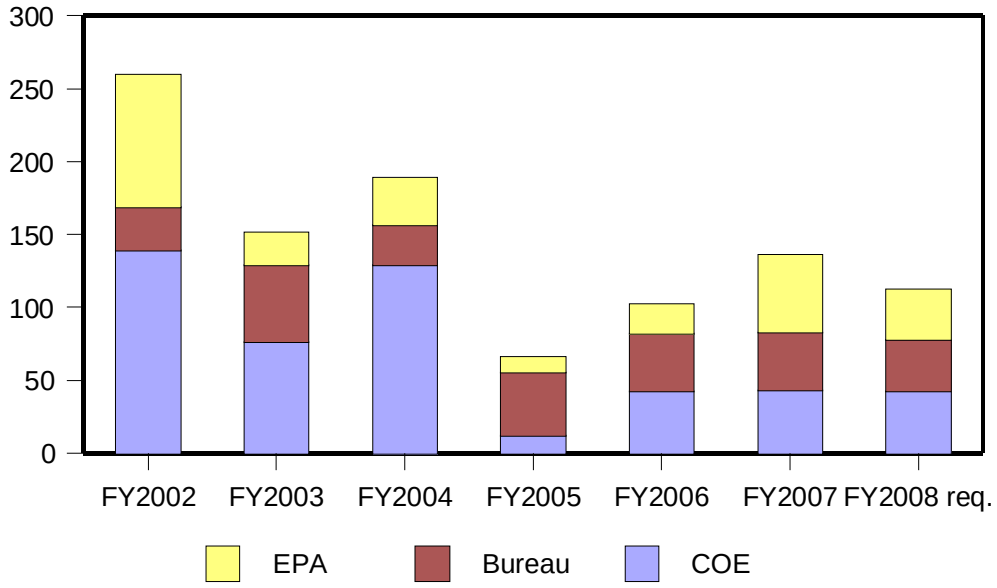
Appropriations. Since the September 11 terrorist attacks, Congress has provided appropriations to the Corps, the Bureau, and EPA for security-related programs and activities to protect water infrastructure, as shown in **Figure 1**. Through FY2007, appropriations have totaled $788.6 million.

For both the Bureau of Reclamation and the Army Corps of Engineers, appropriations immediately after September 11 were intended to support risk assessment of needed security improvements, followed by implementation of measures to ensure the safety and security of the public, Bureau and Corps employees, and the facilities. For example, since FY2004, both agencies have implemented physical hardening and other protective measures, as well as personnel and information security. Both agencies continue to assess and reassess security needs at their facilities as part of ongoing efforts to ensure their long-term security. The Bureau's security budget includes a law enforcement program (guards and surveillance), facility fortification, studies, and review, plus specific amounts

designated for five National Critical Infrastructure (NCI) dam facilities: Hoover, Shasta, Grand Coulee, Glen Canyon, and Fulsom. The Corps' budget as shown in **Figure 1** covers recurring security costs (i.e., guards and monitoring) for its administrative buildings and other general use facilities. The Corps also funds certain project-specific facility security upgrades; these amounts cannot be easily identified in the Corps' budget and are not reflected in the figure.

Funding appropriated to EPA has supported a number of activities. Significant portions of appropriations in FY2002 and FY2003 were for EPA grants for vulnerability assessments carried out by small and medium-size drinking water systems, to assist them in complying with requirements of the Public Health Security and Bioterrorism Preparedness and Response Act (P.L. 107-288; see "Congressional Activity," below). EPA appropriations support training and development of voluntary industry best practices for security and grants to states and territories for coordination activities for critical water infrastructure security efforts ($5 million per year). EPA also provides support for water security information sharing for drinking water and wastewater utilities through the WaterISAC and the Water Security Channel. EPA has supported two special initiatives since FY2006: a pilot program to design, deploy, and test biological or other contamination warning systems at drinking water systems (initially known as WaterSentinel, this activity is now called the water sector initiative), and a related program, the Water Alliance for Threat Reduction (WATR), to train utility operators at the highest risk systems.

Figure 1. Water Infrastructure Security Appropriations
(millions of dollars)



Policy Issues and Congressional Responses

Congress and other policymakers have considered 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 distributed and diverse nature of ownership (federal, non-federal government, and private) complicates assessing and managing risks, as does the reality of limited resources. 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 the September 11 attacks, 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 have examined 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 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 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 Presidential Directive/HSPD-7. This issue arose in 2004 as a result of moves by DHS to carry out its mandates for assessing and protecting critical infrastructure, although EPA remains the lead federal agency for the water sector (see above discussion).

For some time, the two agencies have been working to clarify their roles in providing security to water utilities and in other areas and have negotiated agreements concerning joint research projects and coordination for specific field operations. Nevertheless, in the conference report accompanying the FY2005 Consolidated Appropriations Act, Congress directed EPA to enter into a memorandum of understanding (MOU) with DHS to define the relationship of the two entities with regard to the protection and security of the nation. The memorandum was expected to specifically identify areas of responsibilities and the potential costs (including which entity pays, in whole or part) for meeting such responsibilities.[16] In response, EPA did not enter into a new MOU but instead, in November 2005, issued a report that identified general authorities that govern EPA's and DHS's respective actions, ongoing projects that reflect coordination, and existing project-specific MOUs.

This joint report on roles and responsibilities still may not resolve the growing potential for duplication and overlap among agencies. Currently, for example, policies are being developed both by DHS and EPA, and both agencies are being assisted by separate advisory groups — the Water Sector Coordinating Council works principally with DHS, while EPA has its own Water Security Working Group.

---

[16] H.Rept. 108-792, to accompany H.R. 4818, Consolidated Appropriations Act, 2005, *Congressional Record,* daily edition, November 19, 2004, p. H10850.

Similarly, information sharing and dissemination even in this one sector are occurring through several different mechanisms: DHS supports the Homeland Security Information Network (HSIN), while drinking water and wastewater utilities also may receive security-related advisories from two other sources, the WaterISAC and the Water Security Channel. Some have questioned the multiple advisory groups, on top of existing entities, and in particular the potential that the several mechanisms for sharing homeland security information could transmit inconsistent information and make the exchange of information more complicated, not less. Others are optimistic that the systems and groups will sort themselves out into compatible and complementary networks of information sharing, but that process could take considerable time.

In its March 2006 report, GAO commented on these multiple information services designed to communicate information to the water sector, but also acknowledged EPA's and DHS's ongoing efforts to coordinate their activities to advance water sector security. GAO recommended that DHS and the Water Sector Coordinating Council identify areas where information-sharing networks supported by EPA and DHS (especially the WaterISAC and HSIN) could be better coordinated to avoid operational duplications and overlap and to ensure that security threat information is provided to water systems on a timely basis. Water utility industry groups responded to GAO's recommendation by saying that such coordination efforts are, in fact, underway.

Another information 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 great 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 and utilities generally must pay for improvements using the same revenue or funding sources also needed for other types of capital projects.

Congressional Activity. Since the September 11, 2001 attacks, Congress has 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*, by Mary Tiemann.) 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 six-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 was approved by the House on May 7, 2003, by a 413-7 vote (H.R. 866, identical to H.R. 5169 in the 107th Congress). The Senate Environment and Public Works Committee approved related legislation on May 15, 2003 (S. 1039, S.Rept. 108-149). No further action occurred, due in part to concerns expressed by some that the legislation did not require that vulnerability assessments be submitted to EPA, as is the case with drinking water assessments required by the 2002 Bioterrorism Preparedness Act.

109th Congress. Several aspects of water infrastructure security were debated during the 109th Congress. For example, wastewater security issues again received attention. On May 23, 2006, the Senate Environment and Public Works Committee approved S. 2781 (S.Rept. 109-345). It was similar to S. 1039 in the 108th Congress in that it would have encouraged wastewater utilities to conduct vulnerability assessments and authorized $220 million to assist utilities with assessments and preparation of site security plans. It also included provisions responding to GAO's March 2006 report that found that utilities have made little effort to address vulnerabilities of collection systems, which may be used by terrorists to introduce hazardous substances or as access points for underground travel to a potential target (*Securing Wastewater Facilities, Utilities Have Made Upgrades but Further Improvements to Key System Components May Be Limited by Costs and Other Constraints*, GAO-06-390). S. 2781 would have authorized EPA to conduct research on this topic. During consideration of the bill, the Senate committee rejected an amendment that would have required, rather than encouraged, treatment works to conduct vulnerability assessments and also would have required high-risk facilities to switch from using chlorine and similar hazardous substances to other chemicals that are often referred to as "inherently safer technologies." There was no further action on this legislation, but similar legislation has been introduced in the 110th Congress (S. 1968).

On June 22, 2006, the House Resources Subcommittee on Water and Power held a hearing to review concerns of a number of water supply and power users of Bureau of Reclamation facilities about paying for security costs at these facilities. Since September 11, the Bureau has increased security and anti-terrorist measures at

federal multi-purpose dams. From 2002 through 2004, all of the incremental security costs were paid by the federal government. Project beneficiaries such as irrigation districts, who already generally pay capital costs, as well as operation and maintenance (O&M) costs, for water supply or power generation from these facilities, were not asked to reimburse or pay for added security costs. Beginning in 2005, the Administration requested that the guards and patrols portion of the site security costs be treated as project O&M costs subject to full reimbursement by beneficiaries. Congress declined this request for FY2005, but agreed to make a portion of the costs reimbursable for FY2006 (capped at $10 million, or about one-half of the Bureau's projects costs for guards and patrols in 2006). The FY2007 budget again requested that nearly all costs be reimbursable (i.e., $18.9 million of $20.9 million in post-September 11 costs). At issue at the hearing was whether such costs should be reimbursable, in part or in whole, and whether those who do pay should receive a detailed accounting of activities and facilities that are supported with this funding.

At the hearing, many users argued that security costs for which the general public is the beneficiary, including obligations for national defense, should properly be the federal government's responsibility. Other users would support limited reimbursement, such as the $10 million cap established for FY2006. The issue is especially a concern for beneficiaries of the Bureau's five high-priority dams, such as Hoover and Grand Coulee, which have the largest security needs, because these users are being asked to pay a proportionally higher share of total security costs than users of other Bureau facilities. The Commissioner of Reclamation testified that, in the Administration's view, project beneficiaries have had several years to adjust their expectations, budgets, and planning for current guard and patrol levels and that post-September 11 cost increases should be considered project O&M expenses subject to allocation among project purposes and reimbursement from beneficiaries. In legislation providing the Bureau's FY2007 appropriation (H.R. 5427), the House endorsed the Administration's request concerning reimbursement of site security costs, as did the Senate Appropriations Committee. Because the 109th Congress did not take final action on appropriations for the Bureau before adjourning in December 2006, there was no final action on H.R. 5427. In the 110th Congress, the House Natural Resources Committee has approved a bill (H.R. 1662) that would require water and power users to pay for the cost of security guards, but would set an $18.9 million cap on the amount to be paid by users.

The issue of security of wastewater and drinking water utilities also was debated in connection with legislation dealing with chemical manufacturing plant security. As part of a bill providing FY2007 appropriations for the Department of Homeland Security, Congress included provisions that give DHS authority to establish risk-based and performance-based security standards at the nation's chemical plants (Section 550 of H.R. 5441; P.L. 109-295). Chemical plants are required to conduct vulnerability assessment and create and implement site security plans based on identified vulnerabilities.[17] During consideration of comprehensive chemical plant security bills during the summer of 2006 (S. 2145, H.R. 5695), some had proposed

---

[17] For additional information, see CRS Report RL33043, *Legislative Approaches to Chemical Plant Security*, by Dana Shea.

that water systems (drinking water and wastewater) be included in the legislation because many store or use extremely hazardous substances, such as chlorine gas, that can injure or kill citizens if the chemicals are suddenly released (see page 5). However, water system officials argued that the water sector should be excluded, because facilities have already undertaken vulnerability assessments (as required for many drinking water systems under the 2002 Bioterrorism Act, and as many wastewater utilities have done voluntarily). Further, they argued that requirements in the legislation were potentially duplicative of Risk Management Plan provisions in the Clean Air Act, which apply to more than 2,800 of the largest water utility systems. The chemical plant security provisions in P.L. 109-295 endorsed these arguments and excluded water systems from the new requirements. In July 2007, at a House Homeland Security Committee oversight hearing, DHS Assistant Secretary for Infrastructure Protection Bob Stephan said that the water sector's exclusion from the Chemical Security Act created a "regulatory gap." He said that DHS is reviewing ways to boost safeguards at water utilities that use large amounts of gaseous chlorine, but he did not provide specifics or details.

The results of the 2006 midterm elections and changed congressional leadership led many stakeholders to anticipate more oversight of current homeland security programs and activities and possibly consideration of additional measures in the 110th Congress. For now, it remains unclear whether water infrastructure security will specifically be part of the agenda of future congressional activity.