Order Code RS21026
Updated May 21, 2003

Terrorism and Security Issues Facing the Water Infrastructure Sector

Claudia Copeland and Betsy Cody
Resources, Science, and Industry Division

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 since the September 11, 2001, terrorist attacks. 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. Policymakers are considering a number of options, 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 approved $410 million in funds for security at water infrastructure facilities (P.L. 107-117, P.L. 108-7, and P.L. 108-11) and passed a bill requiring drinking water utilities to conduct security vulnerability assessments (P.L. 107-188). Congress also created a Department of Homeland Security with 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.

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

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

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
21 MAY 2003	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Terrorism and Security Issues Facing the Water Infrastructure Sector	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **David D. Acker Library and Knowledge Respiratory Defense Acquisition University Fort Belvoir, VA 22060**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**6**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

causing loss of life. 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." 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.

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 raw water contaminants; 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 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, Arlington County, and the City of Falls Church. The largest federal 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 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 could cause widespread panic, economic impacts, and a loss of public confidence in water supply systems.

Threats 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 threats could deliver massive contamination by 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. Characteristics 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.[2] 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.

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 is 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.

---

[2] Together, these three facilities make up roughly 70% of the total installed electrical capacity (14,092 megawatts) at Bureau projects throughout the West (28% of hydropower capacity in the West and 16% nationwide).

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 threats or vulnerabilities to the integrity of their operations that have been detected and viable resolutions to problems.

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. 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 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, including development of threat/vulnerability risk assessments and identification of biological and chemical agents of concern.[4]

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 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. 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. Wastewater and drinking water utility organizations are implementing computer software and training

---

[3] "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63." See [http://www.ciao.gov/resource/paper598.html].

[4] Critical Infrastructure Assurance Office. *Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities*. January 2001. See [http://www.ciao.gov/resource/cip_2001_congrept.pdf].

materials to evaluate vulnerabilities at large, medium, and small utility systems, and EPA has provided some grant assistance for vulnerability assessments (discussed below).

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 362 high- and significant-hazard dams and facilities and 58 hydroelectric plants. 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.

A February 2003 White House report (*The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*) presents a strategy for protecting the nation's critical infrastructures and identifies 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 proposes 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. In November, Congress approved a major government reorganization to create a Department of Homeland Security, consolidating all or parts of 22 federal agencies (P.L. 107-297). The new department includes coordination to secure 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 legislation did not transfer Corps or Bureau responsibilities for security protection of dams or EPA's responsibilities to assist drinking water and wastewater utilities.

Appropriations. In September 2001, Congress appropriated $40 billion for recovery from and response to terrorist attacks (P.L. 107-38). 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. EPA awarded $51 million for vulnerability assessment grants to 449 utilities in 2002, averaging $115,000 per utility.

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 signed on April 16 (H.R. 1559), Congress provided an additional $39 million for the Corps and $25 million for the Bureau, for increased security measures at their facilities. The President's FY2004 budget request seeks $74 million for water infrastructure security, including $32.4 million for EPA to support utility vulnerability assessments and the Water ISAC, $13 million for the Corps, and $28.6 million for the Bureau.

Policy Options and Congressional Responses

Congress and other policymakers are considering a number of options 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. Another option is review of existing preparedness plans to ensure that they address newer security concerns.

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 Water ISAC and also of the new 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 new Department will coordinate its activities with ongoing security efforts by other federal agencies and non-federal entities that operate water infrastructure systems.

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.

The 107th and 108th Congresses have considered legislation to address various policy options, including government reorganization, and additional appropriations (discussed above). In May 2002, Congress approved the Bioterrorism Preparedness Act (P.L. 107-288) requiring drinking water systems serving more than 3,300 persons to conduct vulnerability analyses and authorizing grant funding to assist utilities. (For information, see CRS Report RL31294, *Safeguarding the Nation's Drinking Water: EPA and Congressional Actions.)* 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). 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). Legislation authorizing the Bureau to contract with local law enforcement to protect its facilities was enacted (P.L. 107-69). 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, by a 413-7 vote. The Senate Environment and Public Works Committee approved related legislation on May 15 (S. 1039).