Order Code RS21026
Updated February 7, 2002

Terrorism and Security Issues Facing the Water Infrastructure Sector

Claudia Copeland and Betsy Cody[1]
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. Most (especially large facilities) have existing emergency plans and coordination mechanisms; at issue now is whether they are sufficient to address serious terrorist threats. Policymakers are considering a number of options, including enhanced physical security, 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 December Congress approved $345 million in funds for security at water infrastructure facilities (P.L. 107-117), and the House and Senate passed separate versions of bills authorizing new water security programs (H.R. 3178, H.R. 3448, S. 1608). 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.[2] 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. 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

[1] H. Steven Hughes and Steve Stitt also contributed to this report.

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

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 interdependent 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 consumer 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 and aqueducts, 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 over the years, 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. Because of their size and scope, 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 drinking water and wastewater utilities (about 15% of the systems) provide water services to more than 75% of the U.S. population. Arguably, these large systems, located primarily in urban areas, 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 an agent's potential as a biological 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 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.[3] 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 had closed all its facilities to visitors after September 11, although locks and dams remained operational. Many of the closed facilities have reopened in recent weeks.

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 utilities (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. Some have done vulnerability assessments, and others are in progress. 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 terrorism concerns. Thus, it is unclear whether existing plans and coordination mechanisms incorporate sufficient procedures to address serious terrorist threats. Utility officials are reluctant to disclose these confidential plans, since doing so might alert terrorists to vulnerabilities.

---

[3] Together, the 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)[4] 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 are 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 undertake jointly 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 developed 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. EPA also is evaluating water system emergency operation plans. An Information Sharing and Analysis Center (ISAC) supported by an EPA grant has been established under AMWA's leadership to allow for dissemination of early warnings and alerts about threats to the integrity and operation of water supply and wastewater systems.[5] Information may include threats or vulnerabilities that have been detected and viable resolutions. It is expected to be operating in May 2002 and will encompass drinking water supply and wastewater. AWWA and EPA have begun hosting workshops for cities on vulnerability assessments and counterterrorism measures.

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. The Department of Health and Human Services also is conducting related research on hospital and health care operations in response to a chemical or biological incident. 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.[6] This report stated that gaps exist in four major areas.

- 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

---

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

[5] See: [http://www.amwa.net/isac/index.html].

[6] 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/CIAO_Document_Library/final.pdf].

- 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 these plants probably represents more of an environmental threat (i.e., by release of untreated sewage into the environment) than direct threats to life or public health and welfare. Vulnerabilities do exist, however. Damage to a wastewater facility prevents water from being treated and can have impact on downriver water intakes. Destruction of containers that hold large amounts of chemicals at both wastewater and drinking water treatment plants could result in environmental release of toxic chemical agents, such as chlorine gas. Also, large collector sewers could be accessed by terrorist groups for purposes of placing destructive devices beneath buildings or city streets. In response, wastewater utility organizations are implementing computer software and training materials to evaluate vulnerabilities.

At the same time, 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 national emergency preparedness program which assists civilian governments in responding to all regional/national emergencies, including acts of terrorism, as well as assuring continuity of Corps operations. Both agencies participate in the Interagency Committee on Dam Safety (ICODS), which is part of the National Dam Safety Program that is led by the Federal Emergency Management Agency (FEMA).

In P.L. 107-38, Congress appropriated $40 billion for recovery from and response to terrorist attacks. The President is directly allocating $20 billion of this total (none of which has gone to water infrastructure), and in October, 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 (H.R. 3338, H.Rept. 107-350), the DOD and Emergency Supplemental Appropriations Act for FY02, provides the full amounts requested for the Bureau and the Corps and increases funding for EPA to $176 million, including increases for EPA's anthrax decontamination and counterterrorism activities.

The President's FY2003 budget requests $246 million for security at water infrastructure facilities, consisting of $28.4 million for the Bureau, $94 million for the Corps, and $124 million for EPA. The bulk of the EPA funding ($75 million) would be directed at researching building decontamination technology, while $15 million would be for vulnerability assessments at small and medium-size drinking water systems.

Policy Options

Congress and other policymakers may consider 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 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 supply sector, while the majority are not federal. 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) could be to restrict visitor access, including at adjacent recreational facilities, which could raise objections from the public. Some operators of non-federal facilities and utilities are likewise concerned. As a precaution after September 11, the New York City Department of Environmental Protection, which provides water to 9 million consumers, closed its reservoirs indefinitely to all fishing, hiking, and boating and blocked access to some roads. Another option is review of existing preparedness plans to ensure that they adequately address newer security concerns. Ordering such reviews would be easier for federal facilities, but logistical and confidentiality issues arise for the thousands of non-federal systems. EPA does not now have a mandate or authority to require utilities to assess potential vulnerabilities or to take specific actions.

Policymakers also may examine measures that could improve coordination and exchange of information on vulnerabilities, risks, threats, and responses. This could include enhanced functions of the National Infrastructure Protection Center (NIPC), which brings together the private sector and government agencies at all levels to protect critical infrastructure, especially regarding cyber issues; additional support for the water industry ISAC for information-sharing specific to this sector; more support for the existing InfraGard Program of the FBI and NIPC that was designed to help identify and coordinate existing infrastructure protection expertise, both inside and outside the federal government; developing new systems and technology for information-sharing; additional support for the Bureau's site security program and the Corps' National Dam Security and National Emergency preparedness programs; and increased support for and sharing of information through the ICODS program.

A number of research needs could be addressed, including 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 resources for a number of these options and how to direct them at public and private sector priorities.

Until recently, Congress has addressed issues of security concerning the nation's water infrastructure by appropriating funds to support existing programs of EPA, the federal water resource agencies, and others. Congressional oversight is now occurring, as well as consideration of legislation to address various policy options and additional appropriations (discussed above). On December 18, the House approved a bill authorizing a 6-year grant program for research and development on security of water supply and wastewater treatment systems (H.R. 3178). The Senate Environment and Public Works Committee approved a similar bill in November (S. 1593, S.Rept. 107-118). On December 11, the House passed H.R. 3448; it includes authorization of funds for vulnerability analyses and response plans to protect drinking water systems. The Senate passed a separate version of that bill on December 20 but without the water utility provisions and also on that day approved a bill authorizing $50 million in grants for drinking water and wastewater utilities to undertake security measures (S. 1608, S.Rept. 107-119). Earlier, Congress enacted legislation authorizing the Bureau to contract with local law enforcement to protect dams and related facilities (H.R. 2925, P.L. 107-69).