Washington (Mr. BAIRD) for his leadership, and the 46 other cosponsors who have helped shape and advance this legislation. My colleagues on the Committee on Science, including the ranking minority member the gentleman from Texas (Mr. HALL), and the chairman and ranking minority members of the Subcommittee on Environment, Technology, the gentleman from Michigan (Mr. EHLERS) and the gentleman from Michigan (Mr. BARCIA) respectively, approved H.R. 3178 unanimously on November 15.

I also want to thank the chairman of the Committee on Transportation and Infrastructure, the gentleman from Alaska (Mr. YOUNG); chairman of the Committee on Energy and Commerce, the gentleman from Louisiana (Mr. TAUZIN); and the chairman of the Committee on Resources, the gentleman from Utah (Mr. HANSEN), for their suggestions and cooperation in clarifying some of the bill's provisions.

Mr. Speaker, at this point, I enter into the RECORD background materials on H.R. 3178, including the exchange of correspondence between the Committee on Science and the Committee on Energy and Commerce, and the Committee on Transportation and Infrastructure.

PURPOSE OF THE BILL

The purpose of H.R. 3178 is to authorize the Environmental Protection Agency (EPA) to provide assistance for research and development of technologies and related processes to strengthen the security of water infrastructure systems.

BACKGROUND AND NEED FOR THE LEGISLATION

Federal, state and local governments have spent tens of billions of dollars to build the nation's drinking water and wastewater treatment infrastructure. In the coming decades, tens of billions more will be required to maintain that infrastructure and meet the needs of a growing population. What has become clear in recent years and, even more so after the September 11, 2001 attacks, is that while the nation's water infrastructure provides safe and plentiful water to more than 250 million Americans, the system was not built with security from terrorism in mind.

How can the nation respond successfully to this new and daunting challenge? Success will depend on, among other things, focused and sustained research to: (1) Assess potential physical, chemical and cyber vulnerabilities of the system, (2) develop techniques for real-time monitoring to detect threats, (3) conduct research on mitigation, response and recovery methods, and (4) develop mechanisms for widely disseminating and sharing information. H.R. 3178 directly addresses these needs by specifically authorizing water system infrastructure research and development projects and by authorizing funding to carry out this important work.

WATER INFRASTRUCTURE

Approximately 170,000 ''public water systems'' provide water for more than 250 million people in the United States. The Safe Drinking Water Act defines public water system as ''a system for the provision to the public of water for human consumption through pipes or other constructed conveyances, if such system has at least 15 service connections or regularly serves at least 25 individuals . . . and includes collection, treatment, storage, and distribution facilities used primarily in connection with the system.'' Environmental Protection Agency (EPA) regulations recognize two primary types of such systems: (1) ''Community water systems,'' which provide drinking water to the same people year-round; and (2) ''non-community water systems,'' which serve people on a less than year round basis at such places as schools, factories or gas stations.

There are approximately 16,000 municipal sewage treatment works, servicing 73 percent of the U.S. population. Privately owned treatment systems, including septic tanks, serve the remaining population. The Federal Water Pollution Control Act (also known as the Clean Water Act) defines treatment works as ''any devices and systems used in the storage, treatment, recycling, and reclamation of municipal sewage or industrial wastes of a liquid nature . . . including intercepting sewers, outfall sewers, sewage collection systems . . . and any works that will be an integral part of the treatment process.''

THREATS TO DRINKING AND WASTEWATER SYSTEMS

Physical threats to drinking water systems include chemical, biological, and radiological contaminants and disruption of flow through explosions or other destructive actions. Like wastewater treatment systems, drinking water systems may also be at risk because of on-site stockpiles of chemicals that could create fire, explosion, or other hazards. Cyber threats are an increasing concern, given the automated, remote-control nature of most drinking water treatment and distribution systems. Systems are also dependent on other critical infrastructure systems such as energy, telecommunications, and transportation. For example, a water treatment plant that depends on daily deliveries by truck of aluminum sulfate, chlorine, or other chemicals needs an emergency operations plan if such deliveries are interrupted. In recent years, most attention has focused on threats to drinking water systems, particularly to water storage reservoirs.

Wastewater treatment facilities have received increasing attention after the September 11, 2001 attacks. Like drinking water plants, they face physical and cyber threats and other vulnerabilities due to their dependence on other critical infrastructures. Particular attention has also focused on the large volume of liquid chlorine, sulfur dioxide, and other toxic chemicals that may be stored or in use at sewage facilities and the potential for an explosion to create a toxic cloud that could threaten employees and surrounding communities. In addition, some research has occurred with respect to alternative treatment systems and chemicals (such as chlorine bleach or sodium hypochorite in lieu of liquid chlorine).

SECURITY REPORTS AND ACTIONS

There has been increasing, though still limited, attention to infrastructure security in recent years. In response to a 1995 Congressional directive, President Clinton established a Commission on Critical Infrastructure Protection, which issued an October 1997 report, ''Critical Foundations, Protecting America's Infrastructures.'' The report addressed various infrastructure systems, including water, and recommended greater cooperation and communication between government and the private sector.

In May 1998, President Clinton issued President Decision Document 63 (PDD–63), which included the goal of protecting the nation's critical infrastructure from intentional physical and cyber attacks by 2003. Plans by key federal agencies to meet this goal were to be in place by late 1998. The report identified water supply as one of eight critical infrastructure systems requiring attention, specifically focusing on the 330 largest community water systems that each serve more than 100,000 persons. PDD–63 designated EPA as the lead federal agency for interacting with the water supply sector.

EPA responded in late 1998 with a ''Plan to Develop the National Infrastructure Assurance Plan: Water Supply Sector'' to address water infrastructure security. In June 2001, EPA's Inspector General issued a report that credited EPA with achieving a fast start on its efforts, but criticized the agency for missing many important milestones it had set for developing critical infrastructure protections. After the report, and again after the September 11 attacks, the pace of EPA's efforts has accelerated.

To date, EPA has entered into a partnership with the Association of Metropolitan Water Agencies (AMWA) and the American Waters Works Association (AWWA) to reduce the vulnerability of water systems. AWWA's Research Foundation has contracted with the Department of Energy's Sandia National Laboratories to develop vulnerability assessment tools for water systems. EPA has also received appropriations (e.g. $2M in FY 01) for projects with Sandia to pilot test physical vulnerability assessment tools and develop a cyber vulnerability assessment tool. Additional actions (e.g. upgrading security technologies and developing real-time monitoring technologies) on a variety of important security related issues have yet to be completed.

PDD–63 also called for the Federal Bureau of Investigation (FBI) to establish a National Infrastructure Protection Center to provide information sharing and analysis and to coordinate with and encourage private sector entities to establish Information Sharing and Analysis Centers (ISACs). AMWA volunteered to be the Water ISAC coordinator. The purpose of the Water ISAC is to provide to water managers early warnings and alerts about threats to the integrity and operation of water supply and wastewater systems.

While various federal agencies are conducting research on water-related security issues, the January 2001 report of the President's Commission on Critical Infrastructure Protection characterized ongoing water sector research efforts as relatively small with a number of gaps and shortfalls. Four major areas for further research are identified: (1) Threat/vulnerability risk assessments; (2) identification and characterization of biological and chemical agents; (3) establishment of a center of excellence to support communities in conducting vulnerability and risk assessments; and (4) application of information assurance techniques to computerized systems used by water utilities.

Various drinking water system managers and researchers have identified priority areas for research, including: (1) Assessment of physical vulnerabilities including disruption of flow and contamination by chemical, biological, or radiological agents; (2) cyber vulnerabilities including process control equipment, Supervisory Control and Data Acquisitions (SCADA) systems, and other information systems; and (3) vulnerabilities associated with interdependencies with other critical infrastructure sectors such as energy, telecommunications, transportation, and emergency services. Specific research needs include: vulnerability assessment tools; technologies and processes for protecting physical assets and information and process control systems; training, education, and awareness programs; information sharing tools; demonstration projects; real-time monitoring and detection systems; and response and recovery plans.