AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Calendar No. 625

109TH CONGRESS, 2d Session | SENATE | REPORT 109–345

WASTEWATER TREATMENT WORKS SECURITY ACT OF 2006

SEPTEMBER 21, 2006.—Ordered to be printed

Mr. INHOFE, from the Committee on Environment and Public Works, submitted the following

R E P O R T

together with

ADDITIONAL VIEWS

[To accompany S. 2781]

[Including cost estimate of the Congressional Budget Office]

The Committee on Environment and Public Works, to which was referred a bill (S. 2781) to amend the Federal Water Pollution Control Act to enhance the security of wastewater treatment works, having considered the same reports favorably thereon with an amendment and recommends that the bill, as amended, do pass.

GENERAL STATEMENT AND BACKGROUND

The nation's 16,000 publicly owned treatment works (POTWs) serve more than 200 million people, or 70 percent of the U.S. population. POTWs consist of not just the treatment plant but 100,000 major pumping stations, 600,000 sanitary sewers and more than 200,000 miles of storm sewers. The sewer systems could provide an underground network through which terrorists could access and damage the business and population centers of most of the nation's major cities. A terrorist could also impair the wastewater treatment process possibly resulting in the release of toxic chemicals including chlorine gas as well as cause harm to the computerized control systems, pump stations and other parts of the facility. Damage to a wastewater treatment plant could result in significant loss

49–010

of life, environmental damage, and the contamination of surface and groundwater/drinking water supplies.

In 1998, President Bill Clinton issued Presidential Directive 63 designating the Environmental Protection Agency (EPA) as the lead agency responsible for overseeing the security of POTWs. Following the tragic events of September 11, 2001, much more focus was placed on securing the nation's infrastructure from a terrorist attack. Congress created the Department of Homeland Security in 2002 and in December 2003, President Bush issued Homeland Security Presidential Directive 7 reiterating that the EPA is the lead Agency for the drinking water and wastewater sector.

In this capacity, the EPA has provided $10 million since 2002 to address the security needs of the wastewater sector. These funds were used to fund the development and dissemination of several risk assessment methodologies to assist treatment works in assessing their vulnerabilities, including the VSAT developed by the National Association of Clean Water Agencies. In addition, EPA worked with Sandia National Laboratories and the Water Environment Federation to provide training to the owners and operators of wastewater utilities on vulnerability assessments and how to mitigate those vulnerabilities. The Water Environment Federation and the American Society of Civil Engineers are working with EPA to carry out the Water Security Enhancement project which is a series of security guidance documents and voluntary security design standards. In 2003, EPA established the Water Security Division to focus on security at water and wastewater utilities.

EPA assisted in the creation of the Water Information Sharing and Analysis Center (WaterISAC) which is operated by the Association of Metropolitan Water Agencies (AMWA). The Agency has provided $6 million for the operation of the WaterISAC through which security related information is provided to water and wastewater utilities for a nominal fee. The WaterISAC can send urgent threat information to utilities and is available 24 hours per day. Further, EPA and the DHS use the Water Security Channel to provide free information to utilities through a password-protected website. Another means of sharing information developed after 9/11 is the Homeland Security Information Network (HSIN). HSIN critical sector is intended to enhance the protection, preparedness and crisis communication and coordination capabilities of the nation's 17 critical information sectors, including wastewater utilities. DHS is in the process of developing an HSIN for water and water utilities.

DHS has several initiatives underway through which it has addressed security of wastewater utilities. Through its Buffer Zone Protection program, DHS provides grants to reduce specific vulnerabilities at critical infrastructure or key resources by assisting local law enforcement to develop a plan for preventative and protective measures to make an attack by terrorists more difficult. As of October 2005, DHS had reviewed the security at 14 wastewater facilities. Further, DHS has visited several wastewater utilities under its Site Assistance Visits program during which it identifies vulnerabilities and reviews mitigation options.

In August 2005, the Nation was challenged by the Hurricanes Rita and Katrina. Hundreds of wastewater utilities incurred significant damage during the hurricanes. In 2006, the Water Envi-

ronment Federation (WEF) released a report entitled, "Assessment of Reconstruction Costs and Debt Management for Wastewater Utilities Affected by Hurricane Katrina." This report found that the effects of Hurricane Katrina on wastewater facilities in Alabama, Louisiana and Mississippi approaches $1.4 billion, and the cost to repair and rebuild is estimated to be $1.2 billion. The report also estimated a reduction in revenue for affected utilities at about $163 million. In February 2006, several national water associations issued a statement in which they committed to promoting mutual aid agreements which proved critical in assisting some utilities after the Gulf Coast hurricanes. The State of Florida has used mutual aid agreements with great success to help utilities immediately impacted by natural disasters.

The Government Accountability Office has released two reports regarding security at POTWs. In its January 2005 report, GAO asked experts in the water profession to identify key vulnerabilities at POTWs and where Federal funds should be spent if such funds were made available to POTWs to secure their facilities. Ranking the key vulnerabilities from highest to lowest, the experts found the treatment works' collection systems network of sewers; the treatment chemicals; certain key components of the main treatment facility; pumping stations; and the control systems (SCADA)[1] to be the most at-risk. Those areas identified as needing Federal funds if such funds are made available include alternative treatment approaches, improved collaboration among States and cities, completing vulnerability assessments, expanded training opportunities for POTW operators, improving national communication efforts between utilities and key entities responsible for homeland security and hardening of physical assets, among others.

In March 2006, the Government Accountability Office issued a report on security measures taken by wastewater utilities. The GAO's survey of the largest 206 facilities found that many had made significant security improvements. According to the survey, 74 percent of the facilities completed a vulnerability assessment, were in the process of completing a survey or had one underway.[2] Of the 206 who responded, 149 had vehicle gates; 174 had security fences; 160 had redundant power sources; 133 had redundant pumping devices or collection bypass systems, [the following numbers reflect changes made before and after Sept 11] 138 facilities have instituted safeguards for onsite delivery of materials and 112 have additional site lighting.[3] The GAO report clearly indicates that much progress has been made at the nation's largest treatment works. However, the Office also found an area very much in need of assistance. Most of the large utilities had not taken steps to secure their collection systems from intruders or harmful substances. There are significant obstacles to securing these systems that can extend for miles underneath major cities.[4]

---

[1] Government Accountability Office. "Wastewater Facilities Experts' Views on How Federal Funds should be Spent to Improve Security," January, 2005. Page 25.

[2] 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." March 2006. page 14

[3] GAO, 2006. Appendix II, page 33 et seq.

[4] GAO, 2006. page 18.

OBJECTIVES OF THE LEGISLATION

S. 2781 provides a financial incentive to POTWs that have not completed a vulnerability assessment to move forward with development and implementation of an assessment, and provides resources to those who have completed their assessments to address needs identified in those assessments. It authorizes EPA to continue working with nonprofit organizations to improve and distribute vulnerability assessment tools and provide technical assistance to small utilities as they seek to identify and meet their security needs. The bill also authorizes research for the potential threats to a POTW's collection system and how best to protect against those threats.

SECTION-BY-SECTION ANALYSIS

Section 1. Short title

This section provides that the Act may be cited as the "Wastewater Treatment Works Security Act of 2006".

Sec. 2. Wastewater Treatment Works Security

(a) Definition of Vulnerability Assessment

SUMMARY

Creates a new section 222 of the Federal Water Pollution Control Act and defines several terms including a disruption of service event, emergency response plan, site security plan and vulnerability assessment. A disruption of service event (DSE) means a natural disaster or event, or a terrorist attack or other intentional act that substantially disrupts the ability of a treatment works to provide safe and reliable conveyance and treatment of wastewater; disposal of effluent or storage of any potentially hazardous chemical used to treat wastewater; damages critical treatment works infrastructure; results in a substantial harmful effect on the environment; or otherwise poses a significant threat to the public health or safety as a result of damage to the treatment works.

An Emergency Response Plan (ERP) is defined as a plan or set of plans developed by or in cooperation with a treatment works that may include the procedures the treatment works will use when a disruption of service event occurs including procedures for ensuring continued service and protection of the public health and environment. The plan may include a discussion of the means by which the POTW will provide information to the surrounding affected communities as well as the means by which the POTW will limit contamination of public water supplies; address contaminants entering the treatment works or its collection system; secure backup power generation; and any additional means of collecting or treating wastewater. The ERP may include plans conducted in accordance with other Federal statutes that address the elements of an ERP under this statute, or ones that are in existence on the date of enactment that are modified to fit the requirements of this statute.

The bill defines a Site Security Plan as a plan to implement, to the maximum extent practicable, changes at a treatment works based on information contained in the vulnerability assessment.

Finally, this section defines a vulnerability assessment (VA) as an assessment of the vulnerability of a treatment works to a disruption of service event. The VA may include a characterization of the treatment works, including its mission and objective, its customer base, the facilities that comprise the treatment works, including the collection system, the pumping station, the power supply, electronic and computer systems, and chemical containers. It further includes any processes at the treatment works and the assets necessary to achieve the treatment works' objectives. The VA may also include an identification and prioritization of adverse consequences to avoid at the treatment works, including substantial disruptions of service; economic impacts; loss of life; and negative health consequences for staff at the treatment works. The VA may include an identification of adverse consequences to the public health and safety and the environment and natural resources and a determination of critical assets of the treatment works that may be subject to a disruption of service event, including pumping stations, power sources, electronic and computer systems and disinfection processes. Finally, the VA may include an analysis of the qualitative probability of a disruption of service event, whether the disruption of service event is the result of a natural or an intentional occurrence, an evaluation of existing countermeasures relating to the treatment works, and an analysis of current risk relating to the treatment works and the development of a prioritized plan for risk reduction at the treatment works.

DISCUSSION

A disruption of service event is intended to cover both intentional acts of harm and natural disasters. In order to protect a facility against a disruption of service event, a POTW would begin with a vulnerability assessment designed to identify those aspects of the facility most likely to suffer harm during an event and most likely to cause harm to the surrounding community. The POTW could also develop a site security plan which implements the findings of the vulnerability assessment including how the POTW will address the vulnerabilities identified in the VA. An ERP is a critical element the importance of which was highlighted after the Gulf Coast Hurricanes. An ERP details how a POTW will respond to an event, including how the surrounding community would be notified of such an event and how to respond to any harm caused by it.

(b) Grants for Vulnerability Assessments and Security Enhancements

SUMMARY

Authorizes the Administrator to provide grants to a State, municipality, intermunicipal or interstate agency, or privately owned utility that principally treats municipal wastewater to conduct a vulnerability assessment of a publicly owned treatment works; to implement security enhancements described in subsection (c)(1); for the development, expansion, or upgrading of emergency response plans and for the voluntary creation or membership in a mutual aid and emergency preparedness agreement; and for the voluntary creation by a State or network of treatment works of, or voluntary participation by a treatment works in, a mutual aid and emergency

network preparedness agreement developed in accordance with the National Incident Management System established pursuant to Presidential directive number 5 of the Department of Homeland Security.

DISCUSSION

Authorizes grants to conduct vulnerability assessments and address a need identified in the assessment. Grants can also be used for the development, expansion or upgrading of an emergency response plan and site security plan as well as for the voluntary creation or membership in a mutual aid and emergency preparedness agreement. More attention became focused on mutual aid agreements after the Gulf Coast Hurricanes. Florida has had mutual aid agreements in place for years. These are agreements between water and wastewater utilities to assist each other in the event of a natural disaster or terrorist event.[5] Fellow utility operators are among those best qualified to assist another POTW in restoring service and responding to a crisis at the facility after a disruption of service event. While these are locally and State driven agreements, S. 2781 would make eligible for funding the creation of such agreements if the local or State stakeholders determine these agreements are in their best interest.

(c) Grants for Security Enhancements

SUMMARY

Paragraph (1) requires an applicant to certify to the EPA that it has conducted a vulnerability assessment and that the need for which it is seeking funding was identified in the assessment. Upon receiving this certification, the EPA may provide grants to the applicant for specific purposes listed in paragraph (2).

Paragraph (2) establishes a list of security needs for which an applicant may receive funding.

Paragraph (3) prohibits funds from being used for personnel costs and the operation and maintenance of facilities, equipment or systems. It further prohibits the Administrator from requiring an applicant to provide the Administrator with a copy of a vulnerability assessment as a condition of applying for or receiving a grant under this section. This section establishes procedures by which the Administrator can ensure that the POTW is in full compliance with all applicable Federal grant requirements. The Administrator shall work with appropriate law enforcement personnel to incorporate protection of sensitive information into existing protocols for protection of such information. It establishes penalties under the Act if the Administrator or his designee knowingly or recklessly reveals the contents of a vulnerability assessment.

Paragraph (4) reiterates that it is a Federal crime under Section 309(c)(4) of the Clean Water Act to falsely certify information to the Federal Government.

Paragraph (5) protects vulnerability assessments certified to the Administrator under this Act from disclosure under Federal, State and local Freedom of Information Acts or similar statutes.

[5] American Water Works Association. "Utilities Helping Utilities: An Act Plan for Mutual Aid and Assistance Networks for Water and Wastewater Utilities," March 2006. Page 1.

DISCUSSION

A treatment works must certify to EPA that it has conducted an assessment and that one of the enhancements listed in Paragraph (2) is included in the assessment. The bill provides several provisions to ensure that the information contained in an assessment is secure while also providing the Federal Government with the ability to ensure full compliance with applicable Federal laws. In order to minimize access to and exposure of the assessments, the bill prohibits the Administrator from requesting a copy of the document. However, the Administrator may visit the facility to view the assessment to ensure that it has been done and that the POTW is in full compliance with Federal rules applicable to grant recipients. If the POTW certified that it had completed an assessment and in fact did not, the owner or operator can be charged with falsely certifying information and subject to penalties under the criminal code (18 USC 1001) and the Federal Water Pollution Control Act (33 USC 1319). Further, EPA must work with the appropriate law enforcement agencies to incorporate into existing protocols the protection of sensitive information obtained by viewing an assessment. It also establishes penalties if the Administrator or his designees recklessly or knowingly reveals information obtained through the inspection of an assessment. However, nothing in this section would impose any penalties on a POTW operator who shares information with appropriate local and State officials.

This section also exempts the information contained in a vulnerability assessment from the Federal Freedom of Information Act (FOIA) as well as relevant State and local laws. The committee recognizes that information pertaining to the vulnerability of a source to terrorism, and the countermeasures adopted to reduce that vulnerability, is among the most sensitive that any facility can generate. The committee also recognizes the need for the public to know whether a local facility has complied with the law; therefore, the FOIA exemption does not apply to the information in a certification filed under this Act. This subsection also respects the needs of State and local governments to obtain information that they need to coordinate with the Federal Government and facilities, by enabling State and local officials designated by the Secretary to obtain protected information, without concern that they might have to disclose it under their own laws or ordinances.

Most security enhancements not related to personnel or operations and maintenance can be funded through this section, including those identified by the GAO as priorities such as hardening facilities like collection systems, securing pumping stations and switching treatment technologies. A 2005 GAO report indicated the need for Federal funds to assist those treatment works interested in switching technologies. Chlorine is by far the most effective disinfectant available and it is the least expensive. During these times of aging systems, growing Federal regulations and limited resources, cost is an important consideration. While utilities have reported a broad range of costs associated with the change from chlorine to liquid bleach or other approaches, the GAO reported that Washington, DC.'s treatment works, Blue Plains, spent $12.5 mil-

lion to change technologies.[6] Officials with Blue Plains confirmed the numbers in the GAO report. San Jose, CA spent $5 million to switch from gaseous chlorine to sodium hypochlorite. A utility may also identify means to secure chlorine tanks and reduce the amount of material stored onsite, thereby reducing potential threats. It is worth noting that wastewater treatment utilities are often owned and operated by municipal governments. These costs are not insignificant particularly if a utility identifies through the Vulnerability assessment and site security plan the means to secure chlorine tanks and reduce the amount stored onsite sufficient that the facility, determines any threat has been mitigated. The decision to switch is made at the local level with full consideration of all factors including the costs, risks posed by transporting alternative substances and the vicinity of manufacturing facilities. POTWs are already undergoing these evaluations. Currently, 116 of the 206 largest POTWs do not use gaseous chlorine. According to the GAO report, another 20 plan to switch to a technology other than chlorine. Those who continue to use chlorine have taken steps to ensure the chlorine is secure.[7]

(d) Grant Amounts

SUMMARY

Paragraph (1) establishes a Federal-local cost share of 75 percent—25 percent.

Paragraph (2) limits the size of any one applicant to $100,000 per facility.

DISCUSSION

Because securing our Nation's infrastructure against terrorism is a partnership between Federal, State and local Government, this section authorizes a Federal-local cost share. In order to ensure that funds are widely distributed and not absorbed by a few large systems, grants are limited to $100,000.

(e) Technical Assistance for Small Publicly Owned Treatment Works

SUMMARY

Paragraph (1) defines a small publicly owned treatment works as a population of fewer than 10,000 individuals.

Paragraph (2) authorizes the Administrator to, in coordination with the States, provide technical assistance to small treatment works in assessing and addressing their security needs.

Paragraph (3) allows the Administrator to provide grants to nonprofit organizations to assist in accomplishing the purposes of this section.

DISCUSSION

It is critical that small systems, which often have fewer resources at their disposal, have the same level of protection as large systems. Subsection (e) authorizes a technical assistance program for

[6] GAO, 2005. page 40.
[7] GAO, 2006. page 47.

treatment works serving less than 10,000 people. Technical guidance may include the conduct of a vulnerability assessment, emergency response plan, or site security plan, training, technical assistance programs and preliminary engineering evaluations. The Administrator may provide grants to nonprofit organizations with expertise in assisting small systems.

(f) Refinement of Vulnerability Assessment Methodology for Publicly Owned Treatment Works

SUMMARY

Authorizes grants to nonprofit organizations to improve vulnerability assessment methodologies and tools for publicly owned treatment works at no cost to the treatment works.

DISCUSSION

Authorizes the Administrator to provide grants to nonprofit organizations to improve vulnerability assessment methodologies and tools for publicly owned treatment works, including those that are part of a combined public wastewater treatment and water supply system. The grants may be used to develop and distribute assessment software upgrades, improve and enhance critical technical and user support functions, expand libraries of information addressing threats and countermeasures, and implementing user training initiatives. These services are to be provided at no cost to the participants/recipients.

(g) Training Grants

SUMMARY

Paragraph (1) authorizes the Administrator to provide grants to nonprofit organizations to be used in accordance with paragraph (2) to implement a comprehensive training program for treatment works or privately owned utilities that principally treat municipal wastewater.

Paragraph (2) provides for the eligible activities that a grant may be used for including development and implementation of a training program that will assist treatment works in conducting vulnerability assessments, developing emergency response plans, and identifying security enhancements. A grant may also be used to develop and disseminate to treatment works information on best practices for emergency response plans and security enhancements, including operational adjustments and design practices.

Paragraph (3) states that this training and technical assistance provided pursuant to a grant under paragraph (1) shall be provided at no cost to the recipients of the assistance.

DISCUSSION

This section authorizes the Administrator to provide grants to non-profit organizations to develop and implement training programs for wastewater treatment works to help them conduct vulnerability assessments and develop emergency response plans. It would also support training designed to help wastewater treatment plants identify needed security enhancements based on their vulnerability assessments and emergency response plans.

Training programs currently offered by non-profit organizations that assist wastewater treatment plants in assessing their vulnerabilities and developing emergency response plans have been effective in helping many utilities address security and emergency preparedness issues. As part of comprehensive legislation aimed at providing wastewater utilities the financial resources necessary to undertake security and emergency preparedness, a strong training component gives further incentive for wastewater utilities to move forward in this area.

(h) Authorization of Appropriations

SUMMARY AND DISCUSSION

Authorizes $200 million for use in making grants to conduct vulnerability assessments and implement security enhancements under subsection (b); $15 million for technical assistance for small systems; and $1 million annually over 5 years for refinement of vulnerability assessment methodology.

Sec. 3. Research and review

Creates a new section 223 of the Federal Water Pollution Control Act (FWPCA).

(a) Definition of Collection System

SUMMARY AND DISCUSSION

Amends title II of the Federal Water Pollution Control Act by adding a definition of "collection system" as meaning the underground network of sewers, including sanitary and storm water collection lines.

(b) Research and Review

SUMMARY

Authorizes the Administrator, in consultation with appropriate Federal agencies, to research and review, or enter into a contract or cooperative agreement for the conduct of research and review, into (1) the means of providing alternative processes to convey, treat, and dispose of wastewater if a disruption of service event occurs; (2) the means by which the collection system of a treatment works could be used to convey hazardous chemicals or substances (including explosive devices) including a comprehensive analysis of the types of hazardous chemicals, substances, and explosive devices that could be placed in the collection system; and how the system could be secured in response to an intentional harmful act; (3) methods of monitoring the collection system of a treatment works for hazardous chemicals or substances, including explosive devices, and unauthorized entry into the collection system of a treatment works; and (4) treatment technologies, including the affordability, effectiveness, and limitations of each treatment technology.

DISCUSSION

Each POTW has a collection system that consists of the pipes used to carry wastewater from homes and businesses to the treatment works. These pipes are often large enough for an individual

to stand in and they provide an underground roadway beneath most major cities. In its January 2005 report, 42 of the 50 experts on GAO's panel identified the collection system as the most vulnerable asset of a POTW. However, there remain many questions and obstacles on how to effectively secure a collection system. This bill authorizes a research program to identify how a collection system could be used in a terrorist attack, how to identify potential chemicals or explosives that could be placed in a collection system, and how best to mitigate against these risks. It also directs EPA to examine the various POTW treatment technologies to determine their affordability and effectiveness.

(c) Authorization of Appropriations

SUMMARY AND DISCUSSION

Authorization of appropriations—authorizes $5 million a year for fiscal years 2007 through 2011.

LEGISLATIVE HISTORY

During the 107th Congress, Senators Robert Smith and James Jeffords introduced S. 1608, which sought to provide grants to drinking water and wastewater facilities to meet immediate security needs. Senators Jeffords and Smith also introduced S. 1593 which authorized the EPA to provide funds to research institutions to research technologies and processes that address physical and cyber threats to water supply systems, including POTWs. The committee reported the bills on December 10, 2001 and modified versions were incorporated into H.R. 3448, the Public Health and Bioterrorism Preparedness Response Act of 2002 (P.L. 107–188), which was signed into law on June 12, 2002.

During the 107th Congress, the House passed by voice vote, H.R. 5169, the Wastewater Treatment Works Security and Safety Act.

During the 108th Congress, on February 2, 2003, Congressmen Don Young, James Oberstar, Jerry Costello and John Duncan reintroduced H.R. 5169 as H.R. 866, the Wastewater Treatment Works Security Act. The House Committee on Transportation and Infrastructure reported the bill on March 11, 2003 by voice vote. The House of Representatives then passed the bill on May 8, 2003, by a vote of 413–2.

Senator Inhofe and Senator Crapo introduced the Senate companion to H.R. 866 on May 12, 2003. The Senate Committee on Environment and Public Works reported S. 1039 by a vote of 13 to 6 on May 15, 2003.

On May 10, 2006, Senator Inhofe introduced S. 2781, which was cosponsored by Senators Chafee and Murkowski. The bill was read twice and referred to the Senate Committee on Environment and Public Works. S. 2781 included S. 1039 from the 108th Congress with modifications. The committee met on May 23, 2006 to consider the bill. S. 2781 was ordered favorably reported, as amended, by voice vote.

ROLLCALL VOTES

The Committee on Environment and Public Works met to consider S. 2781 on May 23, 2006. An amendment was offered by Sen-

ator Inhofe to add a definition of site security plan, add a training program for POTWs, and combine two eligibilities under subsection (c). The amendment was approved by voice vote. Senator Jeffords offered a complete substitute amendment. Senator Voinovich made a motion to table the Jeffords amendment. The motion passed by a rollcall vote of 10 to 8, with Senators Inhofe, Warner, Bond, Voinovich, Chafee, Murkowski, Thune, DeMint, Isakson, and Vitter voting aye and Jeffords, Baucus, Lieberman, Boxer, Carper, Clinton, Lautenberg, and Obama voting nay.

Senator Boxer then made a motion to table S. 2781. The motion failed by a roll call vote of 8 to 10 with Senators Jeffords, Baucus, Lieberman, Boxer, Carper, Clinton, Lautenberg, and Obama voting aye and Senators Inhofe, Warner, Bond, Voinovich, Chafee, Murkowski, Thune, DeMint, Isakson, and Vitter voting nay. S. 2781 was passed by a voice vote.

REGULATORY IMPACT STATEMENT

In compliance with section 11(b) of rule XXVI of the Standing Rules of the Senate, the committee finds that S. 2781 does not create any additional regulatory burdens, nor will it cause any adverse impact on the personal privacy of individuals.

MANDATES ASSESSMENT

In compliance with the Unfunded Mandates Reform Act of 1995 (Public Law 104–4), the committee finds that S. 2781 would not impose Federal intergovernmental unfunded mandates on State, local, or tribal governments.

COST OF LEGISLATION

Section 403 of the Congressional Budget and Impoundment Control Act requires that a statement of the cost of the reported bill, prepared by the Congressional Budget Office, be included in the report. That statement follows:

S. 2781, Wastewater Treatment Works Security Act of 2006, As ordered reported by the Senate Committee on Environment and Public Works on May 23, 2006

Summary

CBO estimates that implementing S. 2781 would cost about $245 million over the next 5 years, assuming appropriation of the authorized amounts. The funds would be used by the Environmental Protection Agency (EPA) to make grants to States, municipalities, or intermunicipal or interstate agencies to conduct vulnerability assessments at publicly owned wastewater treatment facilities and to undertake security enhancements at such facilities. In addition, the funds would be used by EPA to provide technical assistance to small publicly owned treatment facilities, such as training and engineering evaluations of security measures, and to make grants to nonprofit organizations to conduct self-assessments of security vulnerabilities. This legislation also would authorize funding to support EPA's research related to alternative processes to treat and dispose of wastewater in the event of a disaster.

Enacting S. 2781 could affect direct spending and receipts because the bill would provide for penalties against any individual who recklessly reveals information contained in vulnerability assessments of wastewater treatment facilities. CBO expects that penalties collected under the bill would not be significant because violations of this provision would be rare.

S. 2781 contains an intergovernmental mandate as defined in the Unfunded Mandates Reform Act (UMRA); CBO estimates, however, that the costs of complying with that mandate would not exceed the threshold established in that act ($64 million, adjusted annually for inflation). S. 2781 contains no new private-sector mandates as defined in UMRA.

Estimated Cost to the Federal Government

For this estimate, CBO assumes that the bill will be enacted near the end of 2006. CBO estimates that implementing the bill would cost $245 million over the 2007–2011 period, assuming appropriation of the amounts authorized for each year. Those estimated outlays are based on historical patterns for similar activities. The estimated budgetary impact of S. 2781 is shown in the following table. The costs of this legislation fall within budget function 300 (natural resources and environment).

By Fiscal Year, in Millions of Dollars

	2007	2008	2009	2010	2011
CHANGES IN SPENDING SUBJECT TO APPROPRIATION					
Grants for Wastewater Treatment Security.					
Authorization Level	200	0	0	0	0
Estimated Outlays	10	100	55	30	5
EPA Technical Assistance.					
Authorization Level	15	0	0	0	0
Estimated Outlays	3	8	4	0	0
Grants for Small Publicly Owned Treatment Facilities.					
Authorization Level	1	1	1	1	1
Estimated Outlays	1	1	1	1	1
EPA Research on Wastewater Treatment.					
Authorization Level	5	5	5	5	5
Estimated Outlays	5	5	5	5	5
Total Proposed Changes.					
Authorization Level	221	6	6	6	6
Estimated Outlays	19	114	65	36	11

Estimated Impact On State, Local, And Tribal Governments

S. 2781 contains an intergovernmental mandates as defined in UMRA because it would preempt the application of State and local laws providing for public access to information from vulnerability assessments of wastewater treatment facilities. That preemption constitutes an intergovernmental mandate as defined in UMRA, however, CBO estimates that complying with the mandate would not impose significant costs on State, local, or tribal governments; any costs would be well below the threshold established in that act ($64 million, adjusted annually for inflation).

The bill also would authorize grants that would benefit State and local governments that conduct vulnerability assessments and implement security enhancements of wastewater treatment facilities.

Any costs they might incur, including matching funds, would result from complying with conditions for receiving Federal assistance.

Estimated Impact On The Private Sector

S. 2781 contains no new private sector mandates as defined in UMRA.

Estimate Prepared By: Federal Costs: Susanne S. Mehlman; Impact on State, Local, and Tribal Governments: Lisa Ramirez-Branum; Impact on the Private Sector: Amy Petz.

Estimate Approved By: Peter H. Fontaine, Deputy Assistant Director for Budget Analysis.

ADDITIONAL VIEWS OF SENATORS JEFFORDS, BAUCUS, LIEBERMAN, BOXER, CARPER, CLINTON, LAUTENBERG AND OBAMA

General Statement

In the aftermath of the terrorist attacks of September 11, 2001, it is crucial that we as a Nation take every reasonable action we can to prevent terrorism, create effective response and recovery mechanisms, and find ways to minimize any impacts should an event occur. The Congress has a key role in facilitating these actions by establishing authorities for government agencies, establishing the legal framework in which homeland security improvements will occur, and appropriating adequate funding for the homeland security mission. Protecting our Nation's critical infrastructure is a major piece of our homeland security strategy.

The water sector has been identified as an element in our nation's critical infrastructure since the issuance of Presidential Decision Directive 63 (PDD–63), issued by President Clinton in May 1998, which was the first major governmental action focused on reducing the vulnerability of our nation's critical infrastructure.

The security needs are significant in the water and wastewater sectors. There are over 16,000 publicly owned treatment works in the United States, serving more than 200 million people or 70 percent of the U.S. population. Approximately 1,600 are located near large metropolitan areas. These industrial facilities use large quantities of toxic chemicals, such as chlorine, in their treatment and disinfection processes, and their collection systems run beneath every city and town in America. Chlorine is the most commonly used method of disinfection for wastewater treatment. Chlorine is a very corrosive, hazardous chemical that is fatal in large concentrations. It can also burn the eyes, lungs, and skin. It is stored as a liquid after being cooled. When released, it quickly turns to gas, stays close to the ground, and spreads rapidly. One Department of Homeland Security planning scenario estimates that a chlorine tank explosion could result in 17,500 deaths, 10,000 severe injuries, and 100,000 hospitalizations.[1] In addition, a January 2005 report by the Government Accountability Office (GAO) determined that the release of chlorine is the second highest security risk at wastewater facilities after damage to sewer collection systems.[2]

There are also serious public health risks associated with a disruption or service failure at a wastewater treatment plant. Treatment works clean wastewater that comes from our toilets, showers, and sewers and send it back into our rivers, streams, lakes, and oceans. Those same bodies of water are our drinking water sources.

[1] Planning Scenarios Executive Summaries. The Homeland Security Council. July 2004

[2] Government Accountability Office. "Wastewater Facilities: Experts Views On How Federal Funds Should Be Spent To Improve Security" (GAO–05–165) January 2005.

Without proper treatment, we could see the public health effects of the same type of water-borne disease outbreaks such as cholera that we saw in Iraq in 2003 due to the failure of wastewater treatment plants.

In recent years in this country, we have seen firsthand the impact that a cessation of operations at a drinking water or wastewater plant can have. In Cleveland, Ohio, after the August 2003 blackout, several sewage treatment plants discharged at least 60 million gallons of sewage into the Cuyahoga River, Lake Erie, and their tributaries after the power outage caused the plants pumps and blowers to cease operations. Raw sewage bypassed the treatment process and entered receiving waters untreated. The plants have no back-up power systems. Five Cleveland beaches were closed to swimming to protect against water-borne disease. Cleveland's water system also suffered a hit when 1.5 million customers lost water or water pressure due to power failures at four water plants. The city was under a boil water notice for 4 days. In Detroit, Michigan, after the blackout in August 2003 caused the city's water treatment plants to cease operations, the city was under a boil-water advisory for almost a week.

More recently, we saw the impact of a natural disaster on water infrastructure. A couple of days after Hurricane Katrina in August 2005, EPA estimated that more than 1,220 drinking water and 200 wastewater facilities in Louisiana, Mississippi, and Alabama were affected by flooding. One third of the sewage treatment systems in Mississippi were destroyed or very severely damaged and a month following the event, 22 sewage plants in Louisiana, serving more than a half a million customers, were not operating or operating with difficulty. In 2006, the Water Environment Federation (WEF) released a report entitled, "Assessment of Reconstruction Costs and Debt Management for Wastewater Utilities Affected by Hurricane Katrina." This report found that the effects of Hurricane Katrina on wastewater facilities in Alabama, Louisiana and Mississippi approaches $1.4 billion, and the cost to repair and rebuild is estimated to be $1.2 billion. The report also estimated a reduction in revenue for affected utilities at about $163 million. In the aftermath of Katrina, we believe that a vulnerability assessment, site security plan and emergency response plan would be extremely useful to the Federal Government and local authorities in evaluating a wastewater plant's ability to provide the required level of treatment and the scope of repairs necessary to restore the plant.

We believe that the Congress should take the risk to wastewater treatment plants seriously. Unfortunately, we believe that S. 2781, the Wastewater Treatment Works Security Act, as reported out of committee, provides security for our nation's wastewater infrastructure in name only.

Background

Almost immediately after September 11, 2001, the Committee on Environment and Public Works began working with the water and wastewater industries and the EPA to ensure that the nation's water infrastructure was adequately protected. The committee met with key members of the EPA's security team to review the status of our nation's water infrastructure. Several short-term actions had

already been taken. Based on the recommendations of PDD–63, the EPA and its industry partner, the Association of Metropolitan Water Agencies (AMWA), had already established a communication system: the water infrastructure Information Sharing and Analysis Center (ISAC), designed to provide real-time threat assessment data to water utilities throughout the Nation.

Through this partnership, the EPA and AMWA, in cooperation with Sandia National Laboratory, developed an assessment tool that individual water utilities can use to assess their facilities for potential physical and cyber threats. The committee endorsed the concept of vulnerability assessments with bi-partisan action early in the debate on homeland security. On October 11, 2001, Senators Jeffords (I–VT), Smith (R–NH), Graham (D–FL), and Crapo (R–ID) sent a letter to the President with Representatives Tauzin (R–LA), Dingell (D–MI), Gillmor (R–OH), and Pallone (D–NJ) requesting that the President use a portion of discretionary funds to provide assistance for these assessments to water utilities. No response was received.

Legislative action quickly followed. During the 107th Congress, Senator Jeffords (I–VT) and Senator Smith (R–NH), at that time the chair and ranking member of the committee, introduced S. 1593, the Water Infrastructure Security and Research Development Act, which authorized the U.S. EPA to provide funding to support research projects on critical infrastructure protection for water supply systems. The two leaders of the committee also introduced S. 1608, which sought to provide grants to drinking water and wastewater facilities to meet immediate security needs.

S. 1593, the Water Infrastructure Security and Research Development Act, sought to complement the ongoing work at EPA and in the water industry by focusing on mid- to long-term actions designed to enhance our current water security capabilities. The bill authorized $12 million over 5 years to continue ongoing work called for by PDD–63, conduct research to assess potential threats to our water supply system, and develop solutions to safeguard our water systems against those threats. Projects were intended to address both water and wastewater security needs. S. 1608 focused on short term security needs such as re-keying of doors and locks or installation and maintenance of fencing, gating, or lighting. The committee reported both bills on December 10, 2001.

The provisions of S. 1593 and S. 1608 were modified and incorporated into H.R. 3448, the Public Health and Bioterrorism Preparedness Response Act of 2002 (P.L. 107–188), which was signed into law on June 12, 2002. This Act requires that all community water systems serving a population greater than 3,300 people conduct a vulnerability assessment and prepare an emergency response plan that incorporates the results of the vulnerability assessment. The Act establishes specific deadlines and requires that the vulnerability assessments be submitted to the EPA. It includes extensive information protection requirements at the Agency. The Act authorizes $160 million for fiscal year 2002 and such sums as necessary for fiscal years 2003 through 2005 for these purposes and to address basic security enhancements. Finally, the Act requires the Administrator to review and disseminate information to the drinking water industry on current and future methods of preven-

tion of, detection of, and response to contaminant and supply disruption. Despite the fact that the original Senate bills addressed both water and wastewater needs, the provisions of H.R. 3448 were modified to address drinking water facilities only due to jurisdictional concerns raised by a House committee.

Under the authorities provided by P.L. 107–188, EPA continued its work with AMWA to refine and operate the ISAC. EPA provided $51 million in funding to water utilities in fiscal year 2002, and the Agency partnered with numerous industry associations to develop vulnerability assessment and emergency response plan tools and training tailored for specific applications. EPA has also worked to protect wastewater treatment works in accordance with the EPA Strategic Plan for Homeland Security, issued in September 2002. Since September 11, 2001, EPA has provided $1.1 million to the Association of Metropolitan Sewerage Agencies (AMSA) to develop a wastewater security vulnerability assessment tool. That tool is now available to individual treatment works.

After the Public Health and Bioterrorism Preparedness Response Act of 2002 was enacted without addressing wastewater security, Senator Jeffords introduced S. 3037, the Wastewater Treatment Works Security and Safety Act, on October 3, 2002. S. 3037 mirrors the original provisions of S. 1593 and S. 1608 as well as the modified provisions for drinking water in H.R. 3448. The legislation requires all wastewater utilities to conduct vulnerability assessments and to develop or modify emergency response plans to incorporate the results of the vulnerability assessments. It requires that these documents be presented to the EPA for review, and it includes significant security measures designed to protect this information from unauthorized disclosure. It authorizes $185 million for assistance in completing vulnerability assessments, for immediate security improvements, and for assistance to small treatment works. It authorizes $15 million for research to identify threats, detection methods, and response actions. AMSA endorsed S. 3037 on October 1, 2002. During the 107th Congress, the House passed a wastewater security bill, H.R. 5169, the Wastewater Treatment Works Security and Safety Act. Due to significant differences over the treatment of vulnerability assessments in each bill, the House and the Senate were unable to reach agreement on this issue during the 107th Congress.

In the 108th Congress, on April 3, 2003, Senators Jeffords (I–VT), Graham (D–FL), Lieberman (D–CT), and Lautenberg (D–NJ) introduced the Wastewater Treatment Works Security and Safety Act, S. 779. On May 12, 2003, Senators James Inhofe (R–OK) and Mike Crapo (R–ID) introduced S. 1039, also entitled the Wastewater Treatment Works Security and Safety Act. The committee considered and passed S. 1039 on May 15, 2003.

In the 109th Congress, on November 10, 2005, Senators Jeffords (I–VT), Lautenberg (D–NJ), Boxer (D–CA) and Obama (D–IL) introduced S. 1995, the Wastewater Treatment Works Security Act of 2005. The bill requires all wastewater facilities to conduct vulnerability assessments and to develop or modify site security and emergency response plans to incorporate the results of the vulnerability assessments. Treatment works must certify that alternative approaches, such as using smaller quantities or replacing sub-

stances of concern, were considered in preparing their site security plans. It requires that these documents be submitted to EPA for review and approval and it includes significant security measures to protect this information from unauthorized disclosure. Additionally, the bill authorizes $225 million for assistance in completing vulnerability assessments, site security plans, and emergency response plans; for implementing these plans and security enhancements; for immediate security improvements; and for technical assistance in carrying out these activities. The bill also authorizes $5 million in grants for technical assistance to small treatment works and $5 million in grants for improving vulnerability assessments and tools. Finally, it authorizes $15 million for research and review to identify threats, detection methods and response actions at treatment works.

On May 19, 2006, Senator Biden (D–DE) with Senators Jeffords (I–VT) and Boxer (D–CA) introduced S. 2855, the Community Water Treatment Hazards Reduction Act. This bill would significantly reduce the threat of attack on our nation's wastewater and drinking water facilities. In introducing the bill, Senator Biden cited the fact that there are about 100 facilities that store sufficient quantities of chlorine and other toxic chemicals to threaten between 100,000 and 1,000,000 citizens. The bill would cost about $125 million per year, over 5 years, and would require the EPA to prioritize these facilities on the basis of risk. Upon notification of designation as a high risk water facility, such facilities that serve more than 10,000 people will conduct an options feasibility study of the costs and benefits related to inherently safer technologies (IST) and select an IST where feasible. Beginning with the first tier of high risk facilities, the EPA will award grants, and subject to grant availability, issue orders to facilitate the transition to the selected IST. Facilities that transition to the use of one or more IST after September 11, 2001 but before enactment of this legislation, and would qualify as a high consequence water facility under this bill, would be allowed to participate in the grant program. Water facilities that serve less than 10,000 individuals can opt in if they desire and be eligible for grant funding to transition to the use of one or more ISTs.

On May 10, 2006, Senators Inhofe (R–OK), Chafee (R–RI) and Murkowski (R–AK) introduced S. 2781, the Wastewater Treatment Works Security Act. The committee considered and passed S. 2781 on May 23, 2006. We believe that S. 2781, as it passed the committee, does not fulfill our responsibility to provide the American people with the level of security that is required for our wastewater treatment works.

Discussion

On May 23, 2006, the Committee on Environment and Public Works met to consider S. 2781. Senator Jeffords (I–VT) offered an amendment to S. 2781 that would have required wastewater facilities to conduct a vulnerability assessment, prepare or modify an emergency response plan and site security plan incorporating the results of the vulnerability assessment, and submit these documents to the U.S. Environmental Protection Agency for review and approval. The amendment includes significant security measures to

protect this information from unauthorized disclosure. The amendment authorizes $225 million for assistance in completing vulnerability assessments, site security plans, and emergency response plans; for implementing these plans and security enhancements; for immediate security improvements; and for technical assistance in carrying out these activities. The amendment also authorizes $5 million in grants for technical assistance to small treatment works and $5 million in grants for improving vulnerability assessments and tools. Finally, it authorizes $15 million for research and review to identify threats, detection methods and response actions at treatment works. The amendment also incorporates the provisions of S. 2855 discussed above. Specifically, the amendment would also require EPA to prioritize wastewater and drinking water facilities on the basis of risk. Upon notification of designation as a high risk water facility, such facilities that serve more than 10,000 people will conduct an options feasibility study of the costs and benefits related to inherently safer technologies (IST) and select an IST where feasible. Beginning with the first tier of high risk facilities, the EPA will award grants, and subject to grant availability, issue orders to facilitate the transition to the selected IST. Facilities that transition to the use of one or more IST after September 11, 2001 but before enactment of this legislation, and would qualify as a high consequence water facility under this amendment, would be allowed to participate in the grant program. Water facilities that serve less than 10,000 individuals can opt in if they desire and be eligible for grant funding to transition to the use of one or more ISTs. Grant funding in the amount of $125 million, over 5 years, is authorized for the amendment's IST provisions.

Senator Voinovich (R–OH) offered a motion to table the amendment and it passed by roll call vote with Senators Inhofe (R–OK), Warner (R–VA), Thune (R–SD), Murkowski (R–AK), Isakson (R–GA), Vitter (R–LA), Voinovich (R–OH), Bond (R–MO), Chafee (R–RI), and DeMint (R–SC) voting aye, and Senators Jeffords (I–VT), Boxer (D–CA), Lieberman (D–CT), Obama (D–IL), Clinton (D–NY), Baucus (D–MT), Lautenberg (D–NJ), and Carper (D–DE) voting nay. Senator Boxer then made a motion to table S. 2781 which failed by roll call vote, with 10 Republicans voting nay, 1 Independent voting aye, and 7 Democrats voting aye. S. 2781 was passed by voice vote and reported out of committee.

Without the modifications that were included in the Jeffords amendment, we believe that S. 2781 as passed by the committee provides security to wastewater treatment works in name only. First, S. 2781 does not require the completion of vulnerability assessments, site security plans or emergency response plans. We believe that conducting a vulnerability assessment, addressing the security needs it identifies, and incorporating the results into a facility's emergency response plan and preparing a site security plan are the most basic actions that must be taken in each sector of our nation's critical infrastructure. The need for these mandatory security plans is supported by the findings of two recent GAO reports on wastewater security. In January 2005, GAO released a report ("Wastewater Facilities: Experts' Views on How Federal Funds Should Be Spent to Improve Security," GAO–05–165) that highlights the vulnerability of our nation's wastewater systems and rec-

ommends that we take action to protect them now. The report ranks the release of chlorine as the second highest security risk after damage to sewer collection systems. In March 2006, GAO issued another report on security measures taken by wastewater facilities ("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). GAO surveyed 206 large wastewater facilities to determine how many facilities have completed vulnerability assessments and made security improvements. The Majority's Report discusses this GAO report and states that 74 percent of the facilities surveyed have completed a vulnerability assessment, were in the process of completing some type of security assessment, or had one underway. However, it fails to mention that GAO found that 41 percent of the facilities still use chlorine gas for water disinfection and only half have actually completed vulnerability assessments. GAO's most troubling finding is that few wastewater facilities have addressed the number one vulnerability identified by the GAO in 2005-collection systems security.

Even if facilities complete their assessments and plans, S. 2781 does not require that these documents be submitted to the EPA for review and approval, or that they be available to the Department of Homeland Security (DHS) for purposes of prioritizing and coordinating infrastructure protection efforts. We believe that this is a serious obstacle in the DHS's ability to perform its mission. We believe that providing the results of a facility's vulnerability assessment and its site security and emergency response plans to the Federal Government is a vital step both to ensure that such assessments are completed and implemented in critical infrastructure sectors and to ensure that the Federal Government has all of the information it requires to secure the Nation against a potential terrorist attack. In addition, elected officials in Congress have a Constitutional oversight role over Federal agencies and the laws they implement. Under S. 2781, Congress will not be accountable to the public for the purpose or implementation of this law—Congress will not be able to request or access information from the Federal agencies because the agencies will not have such information.

Under S. 2781 as reported, it is unclear where DHS will get the information they require to complete its national vulnerability assessment and make resource allocation decisions that will increase the level of security in our Nation. It is clear that DHS is likely to receive partial information covering only the subset of the wastewater treatment industry that voluntarily chooses to complete a vulnerability assessment and that voluntarily chooses to share the information they collect with DHS. In fact, under the bill, the EPA is prohibited from requesting a copy of the vulnerability assessment from the wastewater facility, but may visit the facility to view the assessment and ensure that one has been completed. This is likely to make it extremely difficult for the Federal Government, including DHS, to seek this information for any purpose. Without the best, most up-to-date, accurate information available, DHS will be unable to fully perform its mission.

We also disagree with the treatment of information that could be submitted under S. 2781. While we agree that vulnerability assess-

ments and security plans are likely to contain some sensitive information that merits special protection against public disclosure, S. 2781 goes too far and would prevent disclosure of even general documents that contain any information derived from these plans, even if they do not reference any particular facility or vulnerability, and even if they do not contain any information that is actually sensitive. The result would be to impose secrecy on many of the agency's general administrative and policy documents relating to wastewater security, seriously impeding oversight and accountability of the program.

Second, S. 2781 does not require the consideration of, or transition to, safer technologies. In our view, this is irresponsible given what we know about available alternatives. In April 2006, the Center for American Progress conducted a survey of 1,800 chemical plants, including wastewater plants, that no longer report using extremely hazardous substances under the Federal Risk Management Planning program.[3] The survey determined that facilities across the country have switched to safer alternatives from a variety of hazardous chemicals, producing dramatic security and safety benefits at a reasonable cost. Some of the report's findings regarding wastewater facilities include: 114 wastewater facilities reported switching to less acutely hazardous treatment chemicals. These facilities generally replaced chlorine gas with liquid chlorine bleach or ultraviolet light and, as a result of these changes, millions of people are no longer at risk of being exposed to toxic gas from these facilities. For example, the following wastewater plants switched from chlorine gas to liquid bleach and prevented the risk of exposure to toxic gas to the following populations: Blue Plains Wastewater Treatment Plant, Washington, DC, 1.7 million people; Mill Creek Wastewater Treatment Plant, Cincinnati, Ohio, 860,000 people; City of Wilmington Water Pollution Control, Wilmington, Delaware, 560,000 people; and Middlesex County Utilities Authority, Sayreville, New Jersey, 10.7 million people.

Third, S. 2781 also sets up a distinct, and vastly different set of rules for wastewater facilities than drinking water facilities, 40 percent of which are co-located, according to GAO. This simply does not make sense. Congress has a duty to provide for the security of our Nation. S. 2781 simply does not. Five years after the terrorist attacks of September 11, 2001 this gap in our nation's security is reckless. The Majority Report notes that cost is an important consideration in switching technologies and states the costs expended by two wastewater plants to switch from chlorine to sodium hypochlorite: the Blue Plains treatment plant in Washington, D.C., spent $12.5 million and a facility in San Jose, California, spent $5 million. The cost of switching to a safer treatment chemical or technology is not prohibitive. We disagree with the Majority regarding the conversion cost at the Blue Plains plant. According to the report, "Eliminating Hometown Hazards Cutting Chemical Risks at Wastewater Treatment Facilities" by Environmental Defense, the Blue Plains facility spent $500,000 in construction costs to switch.[4]

---

[3] Paul Orum, Center for American Progress. *Preventing Toxic Terrorism How Some Chemical Facilities are Removing Danger to American Communities* (April 2006).

[4] Carol Andress, Environmental Defense. *Eliminating Hometown Hazards Cutting Chemical Risks at Wastewater Treatment Facilities (2003)*

This information was provided by Mike Marcotte, chief engineer at the plant at the time of the conversion. Additional capital expenditures were made at this plant that included upgrades to the liquid bleach facilities. Half of the respondents, that responded and provided cost estimates, to the survey conducted by the Center for American Progress reported spending less than $100,000 to switch to safer alternatives and 87 percent spent less than $1 million. For instance, the City of Wilmington, Delaware Water Pollution Control facility spent $160,000 to switch from chlorine gas to liquid bleach.[5] We believe that the wastewater industry should not be exempt from taking basic precautions to evaluate and address its security needs. Therefore, we believe that S. 2781 as reported from committee fails to ensure that even the most basic steps toward a higher level of security in the nation's critical infrastructure sectors are taken.

We believe that the Federal Government has a responsibility to protect the American people. Without the provisions in the Jeffords amendment, we believe that S. 2781 does not fulfill this responsibility. If S. 2781 is implemented as it passed the committee, the Federal Government will not know if wastewater facilities will voluntarily conduct a vulnerability assessment, if they will voluntarily implement the security needs identified, if the most vulnerable facilities will switch to less hazardous materials for use in treatment, or if they will incorporate the results into their emergency response plans, and there will be no way of finding out. We believe that S. 2781 fails to take responsible, basic steps to protect our wastewater infrastructure security from terrorist attack, putting Americans at risk.

JIM JEFFORDS.
JOE LIEBERMAN.
FRANK R. LAUTENBERG.
BARBARA BOXER.
TOM CARPER.
HILLARY RODHAM CLINTON.
MAX BAUCUS.
BARACK OBAMA.

[5]—Cong. Rec. S4805 (daily ed. May 18, 2006) (statement of Sen. Joseph Biden).

CHANGES IN EXISTING LAW

In compliance with section 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill as reported are shown as follows: Existing law proposed to be omitted is enclosed in [black brackets], new matter is printed in *italic*, existing law in which no change is proposed is shown in roman:

FEDERAL WATER POLLUTION CONTROL ACT

* * * * * * *

TITLE II—GRANTS FOR CONSTRUCTION OF TREATMENT WORKS

SEC. 201. (a) * * *

* * * * * * *

SEC. 221. SEWER OVERFLOW CONTROL GRANTS.

(a) * * *

* * * * * * *

SEC. 222. WASTEWATER TREATMENT WORKS SECURITY.

(a) DEFINITIONS.—In this section:

(1) DISRUPTION OF SERVICE EVENT.—The term 'disruption of service event' means a natural disaster or event, or a terrorist attack or other intentional act, that—

(A) substantially disrupts the ability of a treatment works to provide safe and reliable—

(i) conveyance and treatment of wastewater;

(ii) disposal of effluent; or

(iii) storage of any potentially hazardous chemical used to treat wastewater;

(B) damages critical infrastructure associated with a treatment works;

(C) has a substantial adverse effect on the environment as a result of harm caused to a treatment works; or

(D) otherwise poses a significant threat to public health or safety as a result of harm caused to a treatment works.

(2) EMERGENCY RESPONSE PLAN.—

(A) IN GENERAL.—The term 'emergency response plan' means a plan or set of plans developed by or in cooperation with a treatment works that may include the procedures the treatment works will use when a disruption of service event occurs, including procedures for ensuring continued service and protection of the public health and environment.

(B) INCLUSIONS.—The term 'emergency response plan' includes a plan or set of plans that may describe, for a case in which a disruption of service event occurs—

(i) the means by which a publicly owned treatment works will provide information regarding risks to—

(I) the media;

(II) municipal emergency personnel;

(III) health officials;

(IV) the general public;

(V) Federal and State environmental authorities; and

(VI) other potentially impacted water utilities;

(ii) the means by which a publicly owned treatment works will limit contamination of public water supplies, including temporary treatment and other mitigation measures;

(iii) the means by which a publicly owned treatment works will address contaminants entering the treatment works or its collection system, including any contaminants added by emergency response personnel in responding to a natural disaster or terrorist event;

(iv) the means by which a publicly owned treatment works will secure backup generation if a loss of power accompanies the disruption of service event; or

(v) any additional means of collecting or treating wastewater.

(C) CERTAIN OTHER PLANS.—The term 'emergency response plan' may include—

(i) an emergency response plan conducted in accordance with a Federal statute that addresses each element identified under subparagraphs (A) and (B); and

(ii) an emergency response plan in existence on the date of enactment of this section that is modified to include each element identified under subparagraphs (A) and (B).

(3) SITE SECURITY PLAN.—The term 'site security plan' means a plan to implement, to the maximum extent practicable, changes at a treatment works based on information in a vulnerability assessment to address risks posed by a disruption of service event.

(4) VULNERABILITY ASSESSMENT.—

(A) IN GENERAL.—The term 'vulnerability assessment' means an assessment of the vulnerability of a treatment works to a disruption of service event.

(B) INCLUSIONS.—The term 'vulnerability assessment' may include—

(i) a characterization of the treatment works, including, with respect to the treatment works—

(I) mission and objective;

(II) customer base;

(III) the facilities that comprise the treatment works, including—

(aa) the collection system;

(bb) the pumping station;

(cc) the power supply;

(dd) electronic and computer systems; and

(ee) chemical containers;

(IV) processes; and

(V) assets for achieving treatment works objectives;

(ii) an identification and prioritization of adverse consequences to avoid at the treatment works, including—

(I) substantial disruptions of service;

(II) economic impacts;

(III) loss of life; and

(IV) negative health consequences for staff at the treatment works;

(iii) an identification of adverse consequences to the public health and safety and the environment and natural resources;

(iv) a determination of critical assets of the treatment works that may be subject to a disruption of service event, including—

(I) pumping stations;

(II) power sources;

(III) electronic and computer systems; and

(IV) disinfection processes;

(v) an assessment of—

(I) the qualitative probability of a disruption of service event; and

(II) whether the disruption of service event is the result of a natural or an intentional occurrence;

(vi) an evaluation of existing countermeasures relating to the treatment works; and

(vii) an analysis of current risk relating to the treatment works and the development of a prioritized plan for risk reduction at the treatment works.

(b) GRANTS FOR VULNERABILITY ASSESSMENTS AND SECURITY ENHANCEMENTS.—The Administrator may provide grants to any State, municipality, intermunicipal or interstate agency, or privately owned utility that principally treats municipal wastewater—

(1) to conduct a vulnerability assessment of a publicly owned treatment works;

(2) to implement security enhancements described in subsection (c)(1) and other security enhancements to reduce vulnerabilities identified in a vulnerability assessment;

(3) for the development, expansion, or upgrading of an emergency response plan and site security plan; and

(4) for the voluntary creation by a State or network of treatment works of, or voluntary participation by a treatment works in, a mutual aid and emergency network preparedness agreement developed in accordance with the National Incident Management System established pursuant to presidential directive number 5 of the Department of Homeland Security.

(c) GRANTS FOR SECURITY ENHANCEMENTS.—

(1) PREAPPROVED SECURITY ENHANCEMENTS.—On certification by a State, municipality, intermunicipal or interstate

agency, or privately owned utility that principally treats municipal wastewater that a vulnerability assessment has been completed for a treatment works, and that the security enhancement for which assistance is sought is for the purpose of reducing vulnerabilities of the treatment works identified in the vulnerability assessment, the Administrator may provide grants to the State, municipality, intermunicipal or interstate agency, or privately owned utility under subsection (b)(2) for 1 or more of the uses described in paragraph (2).

(2) USES OF GRANT FUNDS.—The uses referred to in paragraph (1) include—

(A) the purchase and installation of equipment for materials and activities relating to access control, intrusion prevention and delay, and detection of intruders and hazardous or dangerous substances, including—

(i) barriers, fencing, and gates;

(ii) security lighting and cameras;

(iii) metal grates, wire mesh, and outfall entry barriers;

(iv) securing of manhole covers and fill and vent pipes;

(v) installation and rekeying of doors and locks; and

(vi) smoke, chemical, and explosive mixture detection systems;

(B) the conduct of an activity to improve the security for electronic, computer, or other automated systems and remote security systems, including—

(i) controlling access to those systems;

(ii) intrusion detection and prevention; and

(iii) system backup;

(C) participation in a training program, and the purchase of training manuals and guidance material, relating to security; and

(D) the conduct of security screening of employees or contractor support services.

(3) LIMITATIONS.—

(A) USE OF FUNDS.—A grant provided under subsection (b) shall not be used for—

(i) payment of personnel costs; or

(ii) operation or maintenance of facilities, equipment, or systems.

(B) DISCLOSURE OF VULNERABILITY ASSESSMENT.—

(i) IN GENERAL.—Except as provided in clause (ii), as a condition of applying for or receiving a grant under this subsection, the Administrator may not require an applicant to provide the Administrator with a copy of a vulnerability assessment.

(ii) EXCEPTION.—To ensure compliance with any applicable Federal grant requirement, the Administrator or a designee of the Administrator—

(I) may request and view a copy of a vulnerability assessment associated with a grant under this section; but

(II) shall not take possession or control of the copy.

(C) RESPONSIBILITY OF ADMINISTRATOR.—Not later than December 31, 2006, the Administrator, in consultation with appropriate Federal law enforcement and intelligence officials, shall incorporate into existing protocols for protection of sensitive information a method by which the Administrator will protect from unauthorized disclosure vulnerability assessment information viewed by the Administrator or a designee of the Administrator pursuant to subparagraph (B)(ii).

(D) PENALTIES.—

(i) IN GENERAL.—Except as provided in clause (ii), any individual who views a vulnerability assessment, a reproduction of a vulnerability assessment, or any information derived from a vulnerability assessment, pursuant to subparagraph (B)(ii) and who knowingly or recklessly reveals the vulnerability assessment, reproduction, or information other than to the Administrator or an individual designated by the Administrator, or for use in an administrative or judicial proceeding to impose a penalty for failure to comply with this section, shall, on conviction—

(I) be imprisoned for not more than 1 year or fined in accordance with chapter 227 of title 18, United States Code, as applicable to class A misdemeanors, or both; and

(II) be removed from Federal office or employment.

(ii) EXCEPTION.—Notwithstanding clause (i), a designee of the Administrator who is an officer or employee of the United States may discuss with any State or local government official the contents of a vulnerability assessment viewed under this paragraph.

(E) EFFECT OF PARAGRAPH.—Nothing in this paragraph authorizes any person to withhold any information from Congress or any committee or subcommittee of Congress.

(4) FALSE CERTIFICATIONS.—An applicant that knowingly submits to the Administrator a false certification or material statement under this subsection shall be subject to a criminal penalty under section 309(c)(4).

(5) EXEMPTION UNDER FOIA AND RELATED LAWS.—Except for information in a certification under this subsection identifying the system for which the certification is submitted and the date of certification of the system, all information contained in a vulnerability assessment certified by an applicant or derived from a vulnerability assessment under this section shall be exempt from the disclosure requirements under—

(A) section 552 of title 5, United States Code (commonly known as the 'Freedom of Information Act'); and

(B) any State or local law providing for public access to information.

(d) GRANT AMOUNTS.—

(1) FEDERAL SHARE.—The Federal share of the cost of an activity funded by a grant under subsection (b) shall not exceed 50 percent, as determined by the Administrator.

(2) MAXIMUM AMOUNT.—The total amount of grants made under subsection (b) for any publicly owned treatment works shall not exceed $100,000, as determined by the Administrator.

(e) TECHNICAL ASSISTANCE FOR SMALL PUBLICLY OWNED TREATMENT WORKS.—

(1) DEFINITION OF SMALL PUBLICLY OWNED TREATMENT WORKS.—In this subsection, the term 'small publicly owned treatment works' means a publicly owned treatment works that services a population of fewer than 10,000 individuals.

(2) SECURITY ASSESSMENT AND PLANNING ASSISTANCE.—

(A) IN GENERAL.—The Administrator, in coordination with the States, may provide technical guidance and assistance to small publicly owned treatment works for—

(i) the conduct of a vulnerability assessment, emergency response plan, or site security plan; and

(ii) the implementation of security enhancements to reduce vulnerabilities identified in a vulnerability assessment.

(B) INCLUSIONS.—Technical guidance and assistance provided under subparagraph (A) may include technical assistance programs, training, and preliminary engineering evaluations.

(3) PARTICIPATION BY NONPROFIT ORGANIZATIONS.—The Administrator may provide grants to nonprofit organizations to assist in accomplishing the purposes of this subsection.

(f) REFINEMENT OF VULNERABILITY ASSESSMENT METHODOLOGY FOR PUBLICLY OWNED TREATMENT WORKS.—

(1) GRANTS.—The Administrator may provide to nonprofit organizations 1 or more grants to be used in improving vulnerability self-assessment methodologies and tools for publicly owned treatment works, including publicly owned treatment works that are part of a combined public wastewater treatment and water supply system.

(2) ELIGIBLE ACTIVITIES.—A grant provided under this subsection may be used—

(A) to develop and distribute vulnerability self-assessment methodology software upgrades;

(B) to improve and enhance critical technical and user support functions;

(C) to expand libraries of information addressing threats and countermeasures; and

(D) to implement user training initiatives.

(3) COST.—A service described in paragraph (2) that is funded by a grant under this subsection shall be provided at no cost to the recipients of the service.

(g) TRAINING GRANTS.—

(1) IN GENERAL.—The Administrator may provide grants to nonprofit organizations to be used in accordance with paragraph (2) to implement a comprehensive training program for treatment works or privately owned utilities that principally treat municipal wastewater.

(2) ELIGIBLE ACTIVITIES.—A grant provided under paragraph (1) may be used—

(A) to develop and implement a training program to assist treatment works in—

(i) conducting vulnerability assessments using vulnerability self-assessment methodology software;

(ii) developing emergency response plans; and

(iii) identifying security enhancements, including operational adjustments and design practices; and

(B) to develop and disseminate to treatment works information on best practices for emergency response plans and security enhancements, including operational adjustments and design practices.

(3) COST.—Training and technical assistance provided pursuant to a grant under paragraph (1) shall be provided at no cost to the recipients of the assistance.

(h) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated—

(1) $200,000,000 for use in making grants under subsection (b), to remain available until expended;

(2) $15,000,000 for use in providing assistance under subsections (e) and (g); and

(3) to carry out subsection (f), $1,000,000 for each of fiscal years 2007 through 2011.

SEC. 223. RESEARCH AND REVIEW OF COLLECTION SYSTEMS AND TREATMENT WORKS.

(a) DEFINITION OF COLLECTION SYSTEM.—In this section, the term 'collection system' means the underground network of sewers, including sanitary and storm water collection lines.

(b) RESEARCH AND REVIEW.—The Administrator, in consultation with appropriate Federal agencies, shall conduct research and a review, or enter into a contract or cooperative agreement for the conduct of research and a review, of—

(1) means of providing alternative processes to convey, treat, and dispose of wastewater if a disruption of service event (as defined in section 222) occurs;

(2) the means by which the collection system of a treatment works could—

(A) be used to convey hazardous chemicals or substances (including explosive devices), including a comprehensive analysis of the types of hazardous chemicals, substances, and explosive devices that could be placed in the collection system; and

(B) be secured in response to an intentional harmful act;

(3) methods for monitoring—

(A) the collection system of a treatment works for hazardous chemicals or substances, including explosive devices; and

(B) unauthorized entry into the collection system of a treatment works; and

(4) treatment technologies, including the affordability, effectiveness, and limitations of each treatment technology.

(c) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this section $5,000,000 for each of fiscal years 2007 through 2011.

* * * * * * *

○