The Drinking Water Security and Safety Amendments of 2002: Is America's Drinking Water Infrastructure Safer Four Years Later?

Steven D. Shermer[1]

1. J.D., Case Western Reserve University School of Law, 2000; LL.M, George Washington University School of Law, 2006.

INTRODUCTION

Since the devastating events of September 11, 2001, addressing the potential vulnerability of our nation's critical drinking water infrastructure to deliberate attack has become a top-priority.[2] This focus on drinking water security stems from renewed concern following September 11th regarding the undeniably severe consequences of damage to or disruption of these critical infrastructure systems.[3] By definition, maintaining the security of these systems is essential to our nation's safety and welfare; both economic and otherwise.[4] Because of how vitally important these systems are to this country's well-being, drinking water infrastructure security is now "a cornerstone of homeland security."[5]

Responding to the "great outcry" that arose after September 11th demanding better protection from terrorism, Congress took action to secure U.S. drinking water systems against future attacks.[6] In June of 2002, the Drinking Water Security and Safety Amendments (hereinafter the "SDWA Amendments") were passed to address the security of community drinking water sys-

2. *See* Itzchak E. Kornfeld, *Terror In The Water: Threats to Drinking Water And Infrastructure*, 9 WIDENER L. SYMP. J. 439, 482 (2003) ("[S]ince the terrorist acts on Sept. 11, 2001, questions have arisen about the vulnerability of our water systems. . .").

3. *See* Claudia Copeland & Betsy Cody, *CRS Report For Congress: Terrorism and Security Issues Facing The Water Infrastructure Sector* 2 (Feb. 7, 2002), *available at* http://carper.senate.gov/acrobat%20files/RS21026.pdf ("Damage to or destruction of the nation's water supply and water quality infrastructure by terrorist attack could disrupt the delivery of vital human services in this country, threatening public health and the environment, or possibly causing loss of life").

4. *See* USA PATRIOT ACT of 2001 § 1016, 42 U.S.C. § 5195c(e) (2006) (Critical infrastructures are "those systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters"). Other critical infrastructure includes, among other things, telecommunications systems, energy resources and distribution networks, banking and finance networks, transportation, food and wastewater systems, and emergency services.

5. Press Release, Am. Water Works Ass'n, Drinking Water Security in America After 9/11: Homeland Security Report – Water Security Since 9/11 Shows 2 (May 1, 2003) *available at* http://www.AWWA.org/advocacy/pressroom/pr/index.cfm?ArticleID=163 (quoting comments of AWWA President, Lynn Stovall).
(You deleted the footnote citation to the Press Release and cited to the actual report. This is incorrect.) The quote comes from the Press Release. The Full-Report is now at note 12.)

6. *See* Michael P. O'Connor and Celia M. Rumann, *Into The Fire: How To Avoid Getting Burned By The Same Mistakes Made Fighting Terrorism in Northern Ireland*, 24 CARDOZO. L. REV. 1657, 1659 (2003).

tems serving over 3,300 people.[7] Under the SDWA Amendments, these drinking water systems must assess their vulnerability to deliberate attempts to disrupt their ability to provide a safe and reliable supply of drinking water.[8] Emergency Response Plans ("ERPs") incorporating the results of the vulnerability assessments must also be developed.[9] In addition, the SDWA Amendments require research into the methods and means that could be used to disrupt the supply of safe drinking water, as well as methods to detect and respond to contamination incidents.[10]

However, over four years after their passage, it is still uncertain whether the SDWA Amendments have made our drinking water demonstrably safer. A key debate remains over which, if any, of the numerous *potential* threats to drinking water infrastructure are indeed *likely*. Until this issue is resolved, it cannot be known whether current efforts to bolster drinking water security are properly focused.[11] Indeed, if the likelihood of a successful terrorist attack on drinking water infrastructure is remote, the drinking water industry's significant investment to comply with the SDWA Amendments may have been needless.

Other questions remain regarding whether the SDWA Amendments are a necessary, affordable, or effective measure to improve drinking water infrastructure security. The SDWA Amendments mirror other emergency planning requirements imposed under environmental laws with which cash-strapped drinking water facilities must already comply. It is estimated that complying with just the initial requirements of the SDWA Amendments will cost more than $500 million, and water infrastructure funding is severely limited.[12] This estimate does not in-

7. *See* Public Health Security and Bioterrorism Preparedness and Response Act of 2002, Pub. L. No. 107-188 §§ 401- 403, 116 Stat. 594, 682-87 (2002) ("An Act To improve the ability of the United States to prevent, prepare for, and respond to bioterrorism and other public health emergencies") (codified at 42 U.S.C. §§ 300g-j (2006)).

8. *See* 42 U.S.C. § 300i-2(a) (2006).

9. *See* 42 U.S.C. § 300i-2(b) (2006).

10. *See* 42 U.S.C. §§ 300i-3 and 300i-4 (2006).

11. *See* TOXIC TERROR: ASSESSING TERRORIST USE OF CHEMICAL AND BIOLOGICAL WEAPONS 1 (Jonathan B. Tucker ed., 2000) (basing policy choices and legislative action simply on the potential effects of a terrorist attack while neglecting a careful assessment of the actual threat is unsound).

12. AM. WATER WORKS ASS'N, PROTECTING OUR WATER: DRINKING WATER SECURITY IN AMERICA AFTER 9/11 13 (2003), *available at* http://www.AWWA.org/advocacy/pressroom/pr/index.cfm?ArticleID=163 (quoting comments of AWWA President, Lynn Stovall [hereinafter PROTECTING OUR WATER]; Susan Bruninga,

clude the cost of actually implementing the security measures at drinking water facilities needed to address identified vulnerabilities. Money spent complying with the SDWA Amendments' requirements may therefore be better spent on achieving the goals of existing laws concerning drinking and surface water integrity.[13]

To resolve these key issues, the Environmental Protection Agency (hereinafter EPA) must first fulfill its duty under the SDWA Amendments to develop and provide current "baseline information to community water systems. . .regarding which kinds of terrorist attacks or other intentional acts are the probable threats. . ." to such systems.[14] Many drinking water security experts believe that EPA failed to provide adequate "baseline information."[15] This rendered drinking water utilities unable to properly assess their vulnerability to relevant threats. Accordingly, EPA must develop and disseminate improved baseline information regarding the probable drinking water threats the SDWA Amendments were intended to address.

In addition, amendments must be made to the SDWA Amendments in order to better achieve the goal of ensuring a safe and reliable supply of drinking water.[16] First, the SDWA Amendments should be amended to require periodic updates of vulnerability assessments and ERPs. Presently, vulnerability assessments and ERPs never need to be updated. As a result, if proper baseline threat information is eventually developed regarding existing threats to drinking water infrastructure, or new threats emerge, drinking water facilities are not required to take such information into account to update their vulnerability assessments or ERPs.

Treatment Officials, Environmental Advocates Urged to Work Together for System Upgrades, 35 BNA ENV'T REP. 1162 (May 28, 2004) (estimating the funding shortfall for drinking water and wastewater infrastructure upgrades and repairs at between $535 billion to $1 trillion over the next 20 years).

13. *See, e.g.*, Federal Water Pollution Control (Clean Water) Act, 33 U.S.C. §§ 1251-1387 (2006); Public Health Service (Safe Drinking Water) Act, 42 U.S.C. §§ 300f-300j (2006).

14. *See* 42 U.S.C. §§ 300i-2(a)(1) (2006).

15. *See* Memorandum from Jeffrey K. Harris, Director for Program Evaluation, Cross-Media Issues to Tracy Mehan, Assistant Administrator for Water 5 (Sept. 24, 2003) *reprinted in Controlling Bioterror: Assessing Our Nation's Drinking Water Security Hearing Before the Subcomm. on Env't and Hazardous Materials of the House Comm. on Energy and Commerce*, 108th Cong. 26 (2004) ("EPA did not provide adequate threat information") [hereinafter Harris]; *see also* 42 U.S.C. §§ 300i-2(a)(1) (2006).

16. *See* 42 U.S.C. § 300i-2(a)(1) (2006).

Second, EPA should be granted additional regulatory and enforcement authority under the Safe Drinking Water Act ("SDWA") to require corrective action when unacceptable drinking water infrastructure vulnerabilities are identified. The SDWA Amendments do not provide EPA with "broad general authority to require actions to address security concerns."[17] Only when a "threatened or potential terrorist attack" presents an "imminent and substantial endangerment" to public health may EPA use its narrow "emergency powers" to require drinking water operators to take action to address infrastructure vulnerabilities.[18] However, these emergency powers are untested and uncertain in scope. Without broader general regulatory and enforcement authority, the public cannot be assured that "the necessary security enhancements are being taken" by water utilities to address critical drinking water infrastructure threats.[19]

Finally, the vulnerabilities of drinking water systems not regulated by the SDWA Amendments must be addressed. Drinking water systems serving less than 3,300 people, non-community water systems, new drinking water systems constructed after the SDWA Amendments' effective date, and drinking water systems serving populations that expand beyond 3,300 people are not subject to the SDWA Amendments' requirements.[20] These drinking water systems serve millions of people on a daily basis, yet they are among the most vulnerable to deliberate attack and receive the least funding to address security issues.[21] Without a more comprehensive plan to address the security of unregulated drinking water systems, we remain susceptible to many of the same devastating consequences an attack on a larger drinking water system could cause.

---

17. Letter from Christine Todd Whitman, U.S. EPA Administrator, to Congressmen John D. Dingell, Attachment, Response to Question 4 (Apr. 22, 2002) *reprinted in Controlling Bioterror: Assessing Our Nation's Drinking Water Security Hearing Before the Subcomm. on Env't and Hazardous Materials of the House Comm. on Energy and Commerce*, 108th Cong. 73 (2004).

18. *See generally* Varu Chilakamarri, *A New Instrument In National Security: The Legislative Attempt to Combat Terrorism Via The Safe Drinking Water Act*, 91 GEO. L.J. 927 (2003) (discussing SDWA § 1431).

19. *See Controlling Bioterror: Assessing Our Nation's Drinking Water Security Hearing Before the Subcomm. on Env't and Hazardous Materials of the House Comm. on Energy and Commerce*, 108th Cong. 69 (2004) (comments of Rep. Stupak).

20. *See* Chilakamarri, *supra* note 18, at 932-33.

21. Copeland and Cody, *supra* note 3, at 2-3.

Despite these concerns, the SDWA Amendments have helped usher drinking water utilities into "a whole new realm of emergency preparedness."[22] While "[n]o set of legal rules can prevent terrorism. . .," compliance with the SDWA Amendments has ultimately led to a safer drinking water infrastructure and a more knowledgeable and better prepared drinking water industry.[23] With limited revisions, the SDWA Amendments could ensure that meaningful steps are taken to protect drinking water facilities from the "new normalcy" of terrorist threats confronting this country.[24]

I.
WHAT'S AT STAKE? EVERYBODY DRINKS BOTTLED WATER THESE DAYS ANYHOW

A. *The Importance of Water*

While opinions vary about the susceptibility of drinking water infrastructure to terrorist attack, there is far less dispute about this country's need for a "reliable, uninterrupted supply of potable water" of sufficient quantity and pressure.[25] Generally speaking, water is essential for the existence of life on this planet.[26] More specifically, each U.S. citizen "requires about 50 quarts of water per day for drinking, bathing, cooking and other basic needs."[27] Largely because of our safe drinking water supply, the United States has one of "the lowest rates of waterborne disease of any nation."[28] Because of how critically important a steady supply of clean drinking water is to maintaining public

22. PROTECTING OUR WATER, *supra* note 12, at 5.

23. *See* Timothy K. Webster, *The Future of the Chemical and Biological Weapons Conventions*, 16 WTR NAT. RESOURCES & ENV'T 187, 191 (2002).

24. *See* Daniel Eisenberg, *Measuring The Threat*, TIME, Nov. 12, 2001, at 35.

25. *See* Tim De Young & Adam Gravley, *Coordinating Efforts to Secure American Public Water Supplies*, 16 WTR NAT. RESOURCES & ENV'T 146, 147 (2002).

26. *See Hearing on H.R. 3178 and the Development of Anti-Terrorism Tools for Water Infrastructure Before the House Comm. on Science*, 107th Cong. 47 (2001) (statement of Richard G. Luthy, Professor of Civil and Environmental Engineering, Stanford University) [hereinafter *Hearing on H.R. 3178*].

27. Jeffrey Kluger and Andrea Dorfman, *The Challenges We Face*, TIME, Aug. 26, 2002, at A10.

28. PROTECTING OUR WATER, *supra* note 12, at 12 (explaining that "waterborne disease is virtually undetectable in the health statistics of the United States"); *see also* Edward P. Richards, *The Role of Medical and Public Health Services In Sustainable Development*, 32 ENVT'L L. REP. 11299, 11300 (2002) ("[W]aterborne disease outbreaks are [now] rare enough to be headline news.").

health and the well-being of the U.S. economy, drinking water infrastructure is an attractive target for terrorists.[29]

A successful terrorist attack on drinking water supplies could cause dramatic public health and safety consequences.[30] Approximately 265 million Americans rely upon public water systems regulated under the SDWA to provide a safe, reliable, and affordable source of drinking water everyday.[31] Significant numbers of people could be exposed initially, and perhaps secondarily, before an attack on drinking water supplies involving clandestine biological (or certain chemical) contaminants is even suspected.[32] In addition, destruction of or damage to water infrastructure components could result in catastrophic flooding, loss of life, damage to the natural environment, and less availability of water for consumers and essential services.[33] Both water quality and quantity could be put in serious jeopardy from a terrorist attack on water infrastructure systems.[34] Thus, public health could be severely impacted by contaminating or disrupting this country's flow of drinking water.

Statements made by captured terrorist leaders confirm that they understand it is also possible "to disrupt the American economy" by attacking its critical drinking water infrastructure.[35] Aside from the public's obvious need for drinking water, it may be surprising to know that "most treated drinking water is used

29. *See Hearing on H.R. 3178*, *supra* note 26, at 47.

30. *See* NAT'L DRINKING WATER ADVISORY COUNCIL, WATER SECURITY WORKING GROUP FINDINGS vii (2005), *available at* http://www.awwa.org/Advocacy/govtaff/govnew.cfm (discussing six significant system failures that could be caused by an attack on drinking water infrastructure) [hereinafter WATER SECURITY WORKING GROUP FINDINGS].

31. *Hearing on Drinking Water Needs and Infrastructure Before the Subcomm. on Env't and Hazardous Materials of the House Comm. on Energy and Commerce*, 107th Cong. 15 (2002) (statement of Benjamin H. Grumbles, Deputy Assistant Administrator of Water, U.S. Envtl. Prot. Agency).

32. *See* Tara O'Toole et al., *Shining Light on "Dark Winter,"* 34 CLINICAL INFECTIOUS DISEASES 972, 974 (2002) (explaining that "by the time a covert attack is discovered, the disease will already be spreading to the next generation of cases, known as 'second-generation' cases"); *see also* ILSI RISK SCIENCE INSTITUTE, EARLY WARNING MONITORING TO DETECT HAZARDOUS EVENTS IN WATER SUPPLIES 22 (Thomas M. Brosnan ed., 1999) (explaining that commonly monitored indicators of water quality are of little use in the event of intentional contamination of water supplies with microbial pathogens or biotoxins) [hereinafter EARLY WARNING MONITORING].

33. *See* Copeland & Cody, *supra* note 3, at 3.

34. *See* De Young & Gravley, *supra* note 25, at 147.

35. Daniel Klaidman et al., *Al Qaeda in America: The Enemy Within*, NEWSWEEK, June 23, 2003, at 44.

for purposes other than consumption."[36] "[C]lean water is essential for certain key industries to produce power, process food, and manufacture essential products."[37] For example, hospitals and other health care facilities,[38] power plants, firefighting, sanitation, and many other industrial processes are all dependent upon a continuous flow of clean water.[39] Future demand is only going to increase.[40] Facilities reliant upon a steady supply of clean water would be unable to function properly in the face of a catastrophic attack on the nation's water supply and distribution network.[41] As a result, the damage caused by an attack on drinking water facilities would be compounded as the cascading effects rippled through other "interdependent" critical infrastructure sectors.[42] This would have crippling economic effects.

Drinking water systems occupy a ". . .strategic position. . .in keeping the wheels of industry turning and in preserving the health and morale of the American populace."[43] Maintaining a reliable supply of clean drinking water is therefore essential to

36. U.S. ENVTL. PROT. AGENCY, RESPONSE PROTOCOL TOOLBOX: PLANNING FOR AND RESPONDING TO DRINKING WATER CONTAMINATION THREATS AND INCIDENTS, INTERIM-FINAL, MODULE 1: WATER UTILITIES PLANNING GUIDE 13 (2003) [hereinafter RESPONSE PROTOCOL TOOLBOX, MODULE 1]; *see also Hearing on Terrorism: Are America's Water Resources and Environment at Risk, Before the Subcomm. on Water Res. and Env't of the House Comm. on Transp. and Infrastructure*, 107th Cong. 51 (2001), *available at* 2001 WL 1192001 (statement of Ronald L. Dick, Deputy Asst. Director, Counter Terrorism Division and Director of National Infrastructure Protection Center, Federal Bureau of Investigation) (explaining that only 1 to 2% of total water consumption is for drinking and preparation of food).

37. *See* De Young & Gravley, *supra* note 25, at 147.

38. Telephone Interview with Dr. Mark Shermer, Chief Managing Officer, Greater Memphis Dialysis and Transplant Services and Attending Physician, St. Francis Hospital, Memphis, Tennessee (Jan. 10, 2006) (explaining that disrupting the flow of water to dialysis clinics would render them "totally inoperable").

39. PROTECTING OUR WATER, *supra* note 12, at 11-12.

40. *See* De Young & Gravley, *supra* note 25, at 148 (discussing the U.S. Census Bureau's documentation of a 9% increase in the number of water-consuming Americans in the 1990's and a predicted growth of water users from an estimated 270 million people in 2000 to 390 million people in 2050).

41. *See Creating the Homeland Security Department: Consideration of the Administration's Proposal: Hearings Before the Subcomm. on Oversight and Investigations of the House Comm. on Energy and Commerce*, 107th Cong. 238 (2002) (statement of John P. Sullivan, President, Ass'n. of Metro. Water Agencies) [hereinafter *Hearing on Creating the Homeland Security Department*].

42. *See, e.g.*, Nancy Gibbs, *Lights Out*, TIME, Aug. 25, 2003, at 31, 39.

43. *See* De Young & Gravley, *supra* note 25, at 146 (quoting former FBI Director J. Edgar Hoover).

preserving both our public health and our economy.[44] There just isn't enough bottled water to go around.

B. *What Are We Trying to Protect?*

The nation's water system represents one of our greatest engineering accomplishments of the twentieth century.[45] Because of this system, "America has long enjoyed the safest drinking water in the world. . ."[46] Critical water infrastructure components include "surface and ground water sources of untreated water for municipal, industrial, agricultural, and consumer needs; dams, reservoirs, aqueducts, and pipes that contain and transport raw water; treatment facilities that remove raw water contaminants; finished water reservoirs; systems that distribute water to users; and wastewater collection and treatment facilities."[47]

The number of individual assets comprising America's critical drinking water infrastructure is enormous. There are more than 75,000 dams and reservoirs, 160,000 public drinking water systems, 16,000 publicly owned wastewater treatment facilities, tens of thousands of major pumping stations, and over 2 million miles of pipes and aqueducts.[48] These individual assets make up water systems that range from "massive, well-known federal and state irrigation, flood control, and drinking water projects down to part-time single well systems providing water during the tourist season at a campground."[49]

Because of how ubiquitous drinking water system components are throughout the country, terrorists are presented with ". . .an almost infinite array of potential targets."[50] Each of the thousands of individual assets that make up this expansive infrastructure represents a potential vulnerability. Beyond the sheer

---

44. *See* Abe Habib, *Terrorism: Preparing for the New Threat to Public Health in Maine*, ASDWA SECURITY UPDATE (Ass'n of State Drinking Water Adm'rs, Washington, D.C.), Fall 2002, at 5, 5, *available at* http://asdwa.org/pubs/securitynews9-02.pdf ("Drinking water is one of the most important commodities necessary for public health, and protecting that commodity takes precedence over all other initiatives.").

45. *Hearing on H.R. 3178*, *supra* note 26, at 47.

46. PROTECTING OUR WATER, *supra* note 12, at 11; *see also* Richards, *supra* note 5, at 11300 (noting that drinking water sanitation is ". . .responsible for the dramatic increases in life expectancy over the last 150 years. . .").

47. Copeland & Cody, *supra* note 3, at 2.

48. *See id.*; *see also Controlling Bioterror*, *supra* note 19, at 39.

49. De Young and Gravley, *supra* note 25, at 147-48.

50. OFFICE OF HOMELAND SECURITY, NAT'L STRATEGY FOR HOMELAND SECURITY 29 (2002), *available at* http://www.whitehouse.gov/homeland/book/nat_strat_hsl.pdf. [hereinafter NAT'L STRATEGY FOR HOMELAND SECURITY].

numbers, "the realities of the existing infrastructure include unprotected reservoirs, systems with inadequate or no treatment capabilities, minimal real-time quality and pressure monitoring, open distribution systems, aging infrastructure, limited resources. . .and significant growth in demand."[51] Put simply, securing this nation's water infrastructure is a monumental task.

Further compounding these challenges is the lack of integration among the range of entities responsible for operating and maintaining drinking water infrastructure assets. Of the 54,000 community water systems and more than 20,000 non-community water systems, many are municipally owned and operated.[52] However, many private entities and other non-federal units of government are also involved.[53] Not surprisingly, these systems are not well-integrated.[54] Drinking water systems are, ". . .in fact, many thousands of separate infrastructures across the country, with vastly different histories and needs."[55] Consequently, implementing a coordinated plan to address security among the array of entities responsible for overseeing the nation's water infrastructure is an extraordinary challenge.[56]

Because of the "nearly infinite" number of potential drinking water targets, ". . .difficult choices about how to allocate resources against those risks that pose the greatest danger to our homeland. . ." must be made.[57] Unfortunately, "[i]t is impossible to protect completely all targets all the time."[58] The federal government acknowledges that it "do[es] not have enough legs, eyes, and ears to do the job we need to do to prevent and disrupt terrorism."[59] Ultimately, this country may therefore have to accept

51. De Young and Gravley, *supra* note 25, at 148.

52. *Id.*; *see also* PROTECTING OUR WATER, *supra* note 12, at 16-17.

53. *See* Copeland and Cody, *supra* note 3, at 2.

54. *See* De Young and Gravley, *supra* note 25, at 147 (quoting Peter Cook, Executive Director, National Association of Water Companies) ("[t]o think of water infrastructure as integrated on a national level is simply inaccurate").

55. *See id.*

56. *See id.* at 148.

57. NAT'L STRATEGY FOR HOMELAND SECURITY, *supra* note 50, at 3.

58. *Id.* at 29; *see also Hearing on Creating the Homeland Security Department*, *supra* note 41, at 196 (statement of Samuel G. Varnado, Director, Infrastructure and Information Systems Center, Sandia National Laboratory) ("It is unreasonable to expect that every part of the infrastructure can be completely protected. Rather a risk management strategy must be used to decide where to invest limited protection resources").

59. Highlights, *Ridge, Mueller And Top DOJ Officials Address DAS*, 36-AUG PROSECUTOR 8 (2002).

some level of risk to its critical drinking water infrastructure ". . .as a permanent condition."[60]

II.
WHAT ARE WE TRYING TO PROTECT OURSELVES FROM?

The goals of terrorism are simple: to spread panic and cause disruption.[61] By attacking this country's drinking water infrastructure, terrorists could achieve both of these objectives. Since consumers are "highly sensitive" to threats of contamination or disruption, mass panic could be spread even in the absence of an actual attack. "[T]he mere *threat* of contamination" is sufficient to accomplish this goal ". . .if the threat is not properly managed."[62]

Frighteningly, there are a variety of means by which either objective can be carried out. "Drinking water utilities have long been recognized as potentially vulnerable to terrorist attacks of various types, including physical disruption, bioterrorism, chemical contamination, and cyber attack."[63] Furthermore, drinking water systems are vulnerable to radiological contamination, as well as through their dependence upon other critical infrastructure sectors for their proper operation.[64] Terrorists have shown interest in utilizing all of these methods to carry out their insidious goals.[65] Worse yet, "[t]he knowledge, technology, and materials necessary to build weapons of mass destruction are spreading."[66]

---

60. NAT'L STRATEGY FOR HOMELAND SECURITY, *supra* note 50, at 2.

61. *See* Jeffrey Kluger, *Osama'a Nuclear Quest: How Long Will It Take Before al-Qaeda Gets Hold of The Most Dangerous of Weapons?*, TIME, Nov. 12, 2001, at 39.

62. U.S. ENVTL. PROT. AGENCY, WATER SECURITY, BASIC INFORMATION, *at* http://cfpub.epa.gov/safewater/watersecurity/basicinformation.cfm; *see also* U.S. ENVTL. PROT. AGENCY, RESPONSE PROTOCOL TOOLBOX: PLANNING FOR AND RESPONDING TO DRINKING WATER CONTAMINATION THREATS AND INCIDENTS, INTERIM-FINAL, MODULE 2: CONTAMINATION THREAT MANAGEMENT GUIDE 10 (2003) (emphasis added) [hereinafter RESPONSE PROTOCOL TOOLBOX, MODULE 2].

63. *Controlling Bioterror*, *supra* note 19, at 45; *see also* De Young and Gravley, *supra* note 25, at 147 ("The threat of cyber attacks on automated systems used by water utilities should not be underestimated").

64. *See* RESPONSE PROTOCOL TOOLBOX, MODULE 1, *supra* note 36, at 15.

65. Klaidman et al., *supra* note 35, at 42 (explaining that "Al Qaeda chiefs. . .have shown a strong interest in the past in obtaining weapons of mass destruction").

66. NAT'L STRATEGY FOR HOMELAND SECURITY, *supra* note 50, at 9 (stating that "[t]hese capabilities have never been more accessible and the trends are not in our favor").

Since September 11th, we have also unfortunately come to realize that the terrorist organizations likeliest to attempt such attacks are "more global in [their] range, and more ruthless in [their] ideology than all but [their] most dedicated students could have ever imagined."[67] They are strategic actors who "choose their targets deliberately based on the weaknesses they observe in our defenses and our preparations."[68] Furthermore, many terrorist organizations are extremely well-financed.[69] These resources enable terrorists to pursue their most violent objectives by enticing those with technical expertise to help them gain access to mankind's deadliest weapons.[70]

This section examines various means that could be used to attack drinking water infrastructure systems. The most severe characteristics of these weapons are described. Section VI analyzes whether, despite the 'worst case' consequences, these weapons could realistically be used to threaten drinking water infrastructure security, as well as whether other more common threats to the safety of this country's drinking water supplies should be of greater concern.

A. *Biological Weapons:*

"Biological weapons are potentially the most dangerous weapons in the world."[71] They ". . .are composed of agents that are living organisms which infect victims, causing disease, incapacitation, and often death."[72] They also include nonliving toxins extracted from living bacteria, plants, and animals, or synthesized in the laboratory.[73] The threat of bioterrorism has been described as "[a] plague more monstrous than anything we have experienced [that] could spread with all the irrevocability of ink

67. Michael Elliott, *Hate Club*, TIME, Nov. 12, 2001, at 61.

68. NAT'L STRATEGY FOR HOMELAND SECURITY, *supra* note 50, at 7.

69. *See* Jonathan B. Tucker and Amy Sands, *An Unlikely Threat*, 55 BULLETIN OF THE ATOMIC SCIENTISTS 46, 50 (1999) (estimating the Japanese Aum Shinrikyo cult's financial resources at approximately $1 billion and stating that the cult had access to trained scientists).

70. *See* Kluger, *supra* note 61, at 38 (discussing the possible links of one of Pakistan's leading nuclear engineers, Sultan Bashiruddin Mahmood, to al-Qaeda).

71. Remarks on signing the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, 38 WEEKLY COMP. PRES. DOC. 998 (June 17, 2002).

72. Francine M. Guesnier, *World Trade Center Attacks: Fears of Biological Warfare Stand in the Wake*, 2001 COLO. J. INT'L ENVT'L L. & POL'Y 181, 183 (2001).

73. *See* TOXIC TERROR, *supra* note 11, at 4.

on tissue paper."[74] Because of their covert nature and terrible consequences, a terrorist attack involving biological agents raises "nightmares of primal fear."[75]

While information regarding their stability in treated water must be improved, it appears that at least some of the "veritable smorgasbord" of biological warfare agents could be used to threaten water supplies.[76] These include many substances designated by the Center for Disease Control as "Category A" agents based on their high rates of fatality and person-to-person transmission:[77]

- **Anthrax:** Often mentioned as "the biological agent of choice," little information is available about the risks of direct contamination of water with anthrax spores.[78] However, anthrax spores appear to be highly resistant to cold, heat, and chemical disinfectants.[79]
- **Botulinum Toxin:** "Botulinum Toxin is the most poisonous substance known."[80] While it is not contagious, miniscule amounts cause severe health consequences, including death.[81]

---

74. Andrew J. Bacevich, *Bad Medicine for Biological Terror*, 44 ORBIS 221 (2000) (quoting comments of former Secretary of Defense William S. Cohen).

75. Barry Kellman, *Biological Terrorism: Legal Measures For Preventing Catastrophe*, 24 HARV. J. L. & PUB. POL'Y 417, 419 (2001) (describing how "[d]isease—plague, smallpox, and other decimating maladies—is dire trauma embedded in humanity's collective unconscious"); *see also id.* at 429 (". . .humanity fears disease not only for its ability to kill, but for the horrifying way in which it kills").

76. *See* EARLY WARNING MONITORING, *supra* note 32, at 9, *see also id.* at 22; Bacevich, *supra* note 74, at 231.

77. *See* Heather H. Horton et al., *Critical Biological Agents: Disease Reporting As A Tool For Determining Bioterrorism Preparedness*, 30 J.L. MED. & ETHICS 262, 263 (2002).

78. *See generally* Thomas V. Inglesby et al., *Anthrax As a Biological Weapon, 2002*, 287 JAMA 2236, 2238 (2002) (discussing the symptoms, treatments, and health consequences of exposure to anthrax spores).

79. John P. Sullivan, Jr., *The WaterIsac –One Year Later*, 96 AM. WATER WORKS ASS'N J. 1, 32 (Marcia Lacey ed., 2004) (describing the resistance of anthrax to chemical disinfection).

80. *See generally* Stephen S. Arnon et al., *Botulinum Toxin as a Biological Weapon*, 285 JAMA 1059 (2001) (discussing the symptoms, treatments, and health consequences of botulinum toxin poisoning).

81. *See id.* at 1063 (The lethal dose of botulinum toxin is miniscule: "[a] single gram of crystalline toxin, evenly dispersed *and inhaled*, would kill more than 1 million people, although technical factors would make such dissemination difficult"). The *ingested* lethal dose is still tiny – approximately 70 micrograms would kill an average sized person). *See id.*

- **Tularemia:** Tularemia "is one of the most infectious pathogenic bacteria known."[82] "Tularemia's epidemic potential became apparent in the 1930s and 1940s when large waterborne outbreaks occurred in Europe and the Soviet Union."[83]
- **Ricin:** Ricin is a toxin derived from castor beans. It is a stable substance that is not deactivated by extreme conditions such as cold or heat.[84] There is no known treatment for ricin poisoning.[85] Ricin is not contagious; direct contact with the substance is required to be poisoned.[86]
- **Smallpox:** "The smallpox virus is among the most dangerous organisms that might be used by bioterrorists."[87] An infectious dose of smallpox is very small, and once contracted, it is highly contagious.[88] There is no effective therapy to treat smallpox once it is contracted.[89]
- **Plague:** Known as the "Black Death" in the Middle Ages, Plague is a highly contagious bacterial disease that leads to respiratory failure and death.[90] It is only slightly less lethal than anthrax.[91] However, if detected early enough, treatment with antibiotics is effective.[92]
- **Viral Hemorrhagic Fevers:** Viral Hemorrhagic Fevers ("VHF") are a diverse group of organisms, the effects of which (particularly the Ebola virus) provide the inspiration for many of Hollywood's more terrifying portrayals of bi-

---

82. *See generally* David T. Dennis et al., *Tularemia as a Biological Weapon*, 285 JAMA 2763 (2001) (discussing the symptoms, treatments, and health consequences of tularemia).

83. *Id.* at 2764.

84. *See generally* CENTER FOR DISEASE CONTROL, FREQUENTLY ASKED QUESTIONS (FAQ) ABOUT RICIN (2003) (discussing the symptoms and health consequences of ricin poisoning), *at* http://www.bt.cdc.gov/agent/ricin/facts.asp [hereinafter FREQUENTLY ASKED QUESTIONS ABOUT RICIN].

85. *See* Kellman, *supra* note 75, at 437.

86. *See Frequently Asked Questions (FAQ) About Ricin*, *supra* note 84.

87. Kellman, *supra* note 75, at 432; *see also* Guesnier, *supra* note 72, at 183 ("During the twentieth century, smallpox killed more than 500 million people").

88. *See generally* Donald A. Henderson et al., *Smallpox as a Biological Weapon*, 281 JAMA 2127, 2129 (1999) (discussing the symptoms, treatments, and health consequences of smallpox).

89. *See id.* at 2132.

90. *See generally* Thomas V. Inglesby et al., *Plague as a Biological Weapon*, 283 JAMA 2281, 2282 (2000) (estimating that if 110 pounds of aerosolized plague were released over a large city, tens of thousands would be fatally infected).

91. *See* Kellman, *supra* note 75, at 434.

92. *See* Inglesby et al., *supra* note 90, at 2285-86 (discussing the symptoms, treatments, and health consequences of plague).

> oterror incidents.[93] VHF's are generally highly infectious and many are also highly contagious.[94] There are no vaccines to prevent the majority of VHF's.[95] Moreover, very few treatments are effective in for people who already been exposed.[96]

EPA considers other more common biological contaminants as potential threats to drinking water supplies.[97] Given the limited state of knowledge regarding the covert bioweapons programs of certain states, the development of new biological weapons capable of contaminating water supplies cannot be disregarded.[98]

"Bioterrorism presents unique challenges since it differs dramatically from other forms of terrorism and national emergencies."[99] "While explosions or chemical attacks cause immediate and visible casualties, an intentional release of a biological weapon would unfold over the course of days or weeks, culminating potentially in a major epidemic."[100] Initial manifestations

---

93. *See generally* Luciana Borio et al., *Hemorrhagic Fever Viruses as Biological Weapons*, 287 JAMA 2391 (2002) (VHF's include Ebola Virus, Marburg Virus, Lassa Fever Virus, Crimean Congo Virus, Rift Valley Virus, Dengue Fever, Yellow Fever, Omsk Hemorrhagic Fever, and Kyasanur Forest Disease).

94. *See id.* at 2393 (". . .[N]o more than a few virons are required to cause infection" from the Marburg Virus).

95. *See id.* at 2391-92. However, there is an effective vaccine for Yellow Fever. *See id.* at 2400.

96. *See id.* at 2399.

97. *See* RESPONSE PROTOCOL TOOLBOX, MODULE 1, *supra* note 36, at 12-15; *see also* EARLY WARNING MONITORING, *supra* note 32, at 22 (describing a number of other viruses and microbes, including shigella, cholera, salmonella, hepatitis A, and cryptosporidium, that are "well-known waterborne pathogens that have frequently been linked to outbreaks of disease"); *see also* Kornfeld, *supra* note 2, at 469-70 (discussing the potential for cryptosporidium and giardia to affect drinking water supplies).

98. *See generally* Henry Sokolski, *Looming Security Threats: Rethinking Bio-Chemical Dangers*, 44 ORBIS 207, 215-16 (2000) (discussing rumors about the former Soviet Union's development of a new class of biological agents known as "bioregulators"); *see also* JOHN WILHEMI & FRAN KREMER, REPORT IN THE HOMELAND SECURITY WORKSHOP ON TRANSPORT AND DISPOSAL OF WASTES FROM FACILITIES CONTAMINATED WITH CHEMICAL OR BIOLOGICAL AGENTS 6 (Nov. 2003) (explaining that "large scale production processes for biologically active peptides, bioregulators (e.g., histamines), and similar substances is an area rich in potential for weapons").

99. *See* Memorandum from R. Nicholas Palarino, to Members of the Subcommittee on National Security, Veterans Affairs, and Int'l Relations 2 (July 18, 2001), *available at* http://www.house.gov/reform/ns/web_resources/briefing_memo_july_23.htm (quoting Secretary of Health and Human Services, Tommy Thompson).

100. *See id.*; *see also* NAT'L STRATEGY FOR HOMELAND SECURITY, *supra* note 50, at 9 ("Biological weapons are especially dangerous because we may not know immediately that we have been attacked, allowing an infectious agent time to spread.").

of drinking water contaminated with biological agents may simply resemble a naturally-occurring disease outbreak.[101] Until sufficient numbers of people seek medical treatment for symptoms specifically associated with exposure to a biological agent, or the contamination is discovered through monitoring and testing, there may be no indication that a bioterrorist attack has taken place.[102] Because of this time lag, it is particularly difficult to confirm an incident involving biological agents.[103] Existing state, local, and privately owned health care capabilities could be quickly overwhelmed as the effects of a large-scale biological weapons attack spread throughout a community.[104]

Moreover, biological weapons are relatively inexpensive to produce, and the equipment needed to manufacture them ". . .is easy to obtain and conceal."[105] Thus, although there are significant technical challenges to producing biological weapons, these hurdles are not insurmountable.[106]

B. *Chemical Weapons:*

Chemical weapons offer terrorists another option for spreading panic and disrupting domestic water systems. "Chemical warfare (CW) agents are man-made, supertoxic chemicals that can be dispersed as a gas, vapor, liquid, aerosol. . ., or ad-

101. *See Terrorism Preparedness: Medical First Response: Hearing Before the Subcomm. on Nat'l Sec., Veterans Affairs, and Int'l Relations of the H. Comm. on Gov't Reform*, 106th Cong. 51 (1999) (statement of Tara O'Toole explaining that because of the covert nature of a bioterrorist attack, the attack would likely only "come to attention gradually, as doctors became aware of an accumulation of inexplicable deaths among previously healthy people"); *see also* David P. Fidler, *Bioterrorism, Public Health, and International Law*, 3 CHI. J. INT'L L. 7, 10 (2002) ("[F]irst responders in bioterrorist attacks would be the public health and healthcare systems, not firefighters, law enforcement, and emergency-response personnel.").

102. *See* Memorandum from R. Nicholas Palarino, *supra* note 99, at 4.

103. *See* Tucker & Sands, *supra* note 69, at 50 (biological weapons ". . .are well suited to covert delivery"); *see also* Matthew Linkie, Note, *The Defense Threat Reduction Agency: A Note on the United States' Approach to the Threat of Chemical and Biological Warfare*, 16 J. CONTEMP. HEALTH L. & POL'Y 531, 534 (2000) ("[E]ffects may go undetected for minutes (in the case of chemical agents) or for days (in the case of biological agents), making these weapons particularly attractive to terrorists.").

104. *See* NAT'L STRATEGY FOR HOMELAND SECURITY, *supra* note 50, at 43.

105. James G. Hodge, Jr., *Bioterrorism Law and Policy: Critical Choices in Public Health*, 30 J. L. Med. & Ethics 254, 256 (2002). *See also* Kornfeld, *supra* note 2, at 441 (stating that biological weapons are the "poor man's nuclear bomb.").

106. *See* Anthony S. Fauci, *Bioterrorism: Defining a Research Agenda*, 57 FOOD & DRUG L. J. 413, 415-16 (2002); *see also* Hodge, *supra* note 103, at 255 (describing how some of the anthrax involved in the 2001 attacks was processed using sophisticated manufacturing techniques).

sorbed. . .to create 'dusty agents'."[107] They are widely feared for their ability to kill and injure. "[T]he ability of persistent agents such as mustard or VX to contaminate buildings and people creates [an additional] potential for sowing disruption and chaos."[108] There is mounting evidence that terrorist organizations have chemical weapons in their possession and have been training to conduct attacks with them.[109]

There are several basic classes of chemical agents.[110] Choking agents, such as chlorine, damage lung tissue.[111] Blood agents, such as hydrogen cyanide, interfere with cellular respiration.[112] Blister agents, such as mustard gas, cause severe chemical burns to the skin and lungs.[113] Finally, and perhaps the most feared, nerve agents, such as sarin and VX, ". . .attack the central nervous system, resulting in seizures, loss of voluntary control, and a gruesome death by respiratory paralysis."[114] Recent research indicates that VX, sarin, and cyanide may be among the most viable chemical threats to water supplies.[115]

New classes of chemical agents, about which little is known, have also apparently been developed.[116] A variety of less exotic substances, such as industrial chemicals, fuels, pesticides, arsenic, and even nicotine are also all considered to be potential chemical agents.[117] In addition, as discussed below, conventional bombs could cause a *de facto* chemical attack by destroying the chlorine disinfectant storage tanks present at many drinking water facilities.[118]

---

107. TOXIC TERROR, *supra* note 11, at 3.

108. Tucker & Sands, *supra* note 69, at 50.

109. *See* Romesh Ratnesar & Douglas Waller, *Did al-Qaeda Do This?*, TIME, Aug, 26, 2002, at 21 (discussing U.S. intelligence reports that Osama Bin Laden tested nerve agents in the early 1990's while living in the Sudan).

110. *See* TOXIC TERROR, *supra* note 11, at 3.

111. *See id.*

112. *See id.*

113. *See id.*

114. Tucker & Sands, *supra* note 69, at 49-50 (explaining that sarin can "kill in minutes").

115. *See* Pat Phibbs, *EPA Working With Army Chemical Center On Homeland Security Research Projects*, 35 BNA ENV'T REP. 1117 (May 21, 2004).

116. *See* Sokolski, *supra* note 98, at 215-16 (discussing the former Soviet Union's development of a lethal and persistent family of binary chemical weapons known as *Novichok* agents); *see also* EARLY WARNING MONITORING, *supra* note 32, at 8.

117. *See* WILHEMI & KREMER, *supra* note 98, at 4.

118. *See* Chilakamarri, *supra* note 18, at 927 (discussing the potential for a toxic cloud of chlorine gas to be released, potentially injuring or killing thousands); *see also* ASS'N OF METROPOLITAN SEWERAGE AGENCIES, ASSET BASED VULNERABIL-

In addition to their lethality, chemical weapons are also "relatively easy to manufacture, using basic equipment, trained personnel, and precursor materials that often have legitimate dual uses."[119] However, as with biological agents, the effectiveness of using chemical weapons to contaminate drinking water supplies varies considerably.[120] Nevertheless, at least some chemical agents may remain stable in water long enough to create potential public health consequences.[121]

C. *Nuclear/Radiological Weapons:*

It is possible to contaminate drinking water supplies with radiological dispersal devices.[122] Use of such devices against drinking water infrastructure has the potential to ". . .cause fear, injury, and possibly lead to levels of contamination requiring costly and time-consuming cleanup efforts."[123] The prospect of rogue nukes in the hands of terrorists make Anthrax, VX, and explosives look like "little more than a murderous tease. . . ."[124] However, radiological threats against drinking water infrastructure involving smaller-scale "suitcase nukes"[125] and "dirty bombs" seem to currently pose the most likely threat.[126] The materials needed to create dirty bombs are widely used, and sometimes poorly safeguarded.[127]

Terrorists have demonstrated consistent interest in using radiological weapons against the United States. "It's been an open secret in the intelligence community that [Osama] bin Laden and

---

ITY CHECKLIST FOR WASTEWATER UTILITIES 3 (2002), *available at* www.amsa-cleanwater.org/pubs/2002avcheck.pdf.

119. NAT'L STRATEGY FOR HOMELAND SECURITY, *supra* note 50, at 9.

120. TOXIC TERROR, *supra* note 11, at 3 ("Chemical agents vary greatly in toxicity and persistence").

121. *See* RESPONSE PROTOCOL TOOLBOX, MODULE 1, *supra* note 36, at 12.

122. *See id.* at 12-15; *see also* EARLY WARNING MONITORING, *supra* note 32, at 9.

123. Bill Gertz, *CIA Says Al Qaeda Ready To Use Nukes*, WASHINGTON TIMES, June 3, 2003, at A1 (quoting an internal CIA report).

124. Kluger, *supra* note 61, at 39.

125. *See id.* at 40 ("During the cold war, the Soviets built an unknown number of portable nuclear explosives, small enough to be carried in a case 8 in. by 16 in. by 24 in.", 134 of which were lost by the Soviet government, according to a former Russian general.)

126. *See id.* ("Because the [dirty] bomb[s] would require no special skill to build, it's perhaps the most feared of the terrorists' nuclear choices").

127. *See* Gertz, *supra* note 123, at A1 (explaining that many types of such materials are used in hospitals, universities, factories, construction companies, and laboratories).

his al-Qaeda organization have long lusted after nukes."[128] Moreover, the risk of radioactive material falling into the wrong hands is high: "Russia and the former Soviet Union are leaking like a sieve."[129] U.S. nuclear facility security may not be much better.[130] Consequently, nuclear and radiological weapons pose a credible threat to drinking water supply security.

D. *Cyber Attack:*

It is no longer news that ". . .the lives and physical security of citizens are becoming increasingly dependent upon mission-critical computer systems, such as those that operate. . .water supplies."[131] However, this dependence has exposed ". . .more numerous and diverse vulnerabilities to terrorists and criminals."[132] Terrorists can now carry out cyber-attacks that "manipulate and exploit a computer system, alter or steal data, or force the computer to perform a function for which it was not meant."[133] Indeed, the use of cyberspace for terrorist purposes stems from military use of technology to wage "Information Warfare" in which ". . .traditional military goals, such as destroying enemy infrastructure targets" are accomplished without a shot being fired.[134] This potential to wreak havoc makes cyberspace an "essential tool" for terrorists.[135] "Although it lacks the doomsday shadow of bio-chemical terrorism or the cataclysmic roar of nuclear terrorism. . .[t]he destruction or temporary denial

128. Kluger, *supra* note 61, at 39 ("Whatever bin Laden's got, he has made any number of attempts to get more"); *see also* Gertz, *supra* note 123, at A1.

129. Kluger, *supra* note 61, at 40 ("Russia's internal-security agencies admit that on hundreds of occasions they have had to seize fissionable materials or technical documents that have fallen into the wrong hands . . . [and] the Atomic Energy Agency reports 175 cases of trafficking in nuclear material since 1993.").

130. *See* John R. Burroughs et al., *Arms Control and National Security*, 36 INT'L LAW 471, 473 (2002).

131. Henry H. Perritt, Jr., *Jurisdiction In Cyberspace*, 41 VILL. L. REV. 1, 120 (1996).

132. *Id.* at 119.

133. *Id.*

134. Jason Barkham, *Information Warfare And International Law On The Use Of Force*, 34 N.Y.U. J. INT'L L. & POL. 57, 60 (2001) (explaining the serious proliferation concerns of non-state actors acquiring IW capabilities with which they could cause serious damage).

135. *See* Susan W. Brenner & Marc D. Goodman, *In Defense of Cyberterrorism: An Argument for Anticipating Cyber-Attacks*, 2002 U. ILL. J. L. TECH. & POL'Y 1 (2002).

of computer system control over. . .essential services[, such as drinking water systems,] would have tragic effects. . ."[136]

Drinking water utilities' increasing reliance upon computerized Supervisory Command and Data Acquisition ("SCADA") systems for managing key facility operations is consequently another prominent vulnerability.[137] "SCADA systems allow utility companies and municipalities to monitor and direct equipment at unmanned facilities from a central location."[138] Dedicated communications channels provide control centers with electronic access to hundreds of 'remote terminal units' that control such diverse operations as water pumping and storage, water treatment operations, and water transmission.[139] A hacker breaking into a SCADA system could therefore hypothetically modify water quality detection systems, steal sensitive information, and prevent or disrupt water deliveries.[140] "Although [the automated] operations are backed up by manual controls, "great damage could be done if the control of these systems was lost for a period of time due to cyber attack."[141]

SCADA systems have been recognized for some time as ". . .highly vulnerable to cyber attack."[142] Unfortunately, according to the FBI, terrorists have sought information about SCADA

---

136. Perritt, *supra* note 131, at 119-20; *see also* Yonah Alexander, *Terrorism in the Twenty-First Century: Threats and Responses*, 12 DEPAUL BUS. L. J. 59, 86 (1999) ("[H]ostile low-risk perpetrators launching a well-coordinated attack with about thirty computer experts strategically placed around the globe and with a budget of approximately 10 million dollars, could bring the United States. . .to its knees.").

137. *See* GOVERNMENT ACCOUNTABILITY OFFICE, DRINKING WATER: EXPERTS' VIEWS ON HOW FEDERAL FUNDING CAN BEST BE SPENT TO IMPROVE SECURITY 9 (2004) *reprinted in Controlling Bioterror: Assessing Our Nation's Drinking Water Security Hearing Before the Subcomm. on Env't and Hazardous Materials of the House Comm. on Energy and Commerce*, 108th Cong. 49 (2004); *see also* Copeland & Cody, *supra* note 3, at 3 ("Cyber attacks on computer operations can affect an entire infrastructure network. . .").

138. Kevin Poulsen, *FBI Issues Water Supply Cyberterror Warning* (January 30, 2002), *at* http://www.securityfocus.com/news/319. SCADA systems are used in other critical infrastructure sectors, such as the electrical power industry.

139. *See id.*; *see also Hearing on H.R. 3178*, *supra* note 26, at 50 ("essentially every component of the water supply system is highly automated").

140. De Young & Gravley, *supra* note 25, at 147.

141. *Hearing on H.R. 3178*, *supra* note 26, at 50.

142. *See Hearing on Creating the Homeland Security Department*, *supra* note 41, at 195-96 (statement of Samuel G. Varnado) ("[I]t is possible to covertly and easily take over control of one of these systems and cause disruptions with significant consequences."); *see also* Poulsen, *supra* note 138 (discussing findings in 1997 that "[c]yber vulnerabilities include the increasing reliance on SCADA systems for control of the flow and pressure of water supplies.").

networks for drinking water facilities.[143] A primary reason for their vulnerability is that drinking water SCADA systems were "generally. . .designed and installed with little attention to security."[144] Existing drinking water facilities were commonly designed with "[p]hysical and electronic single points of failure [that] can easily lead to complete disabling of a SCADA system."[145] Oftentimes, even ". . .new systems are not designed with security in mind."[146] "As a result, many of these networks may be susceptible to attacks and misuses. . ."[147]

As the trend toward downsizing and automation of drinking water facilities accelerates, ". . .SCADA systems will increasingly be exposed to cyber threats."[148] Because the internet is being used more frequently as the means to control SCADA systems, ". . .water systems are more likely to encounter denial of service attacks, viruses, and other malicious programs, which could severely disrupt the operation of these systems."[149] Consequently, the threat of cyber attacks on drinking water infrastructure SCADA systems is a top security concern.[150]

E. *Conventional Weapons:*

Water supply infrastructure has "long been recognized as being potentially vulnerable to terrorist attack. . .including [by] physical disruption."[151] A well-placed bomb could destroy key water infrastructure components causing severe flooding, loss of

143. *See* Poulsen, *supra* note 138.

144. *Hearing on Creating the Homeland Security Department*, *supra* note 41, at 195 (statement of Samuel G. Varnado); *see also* Patricia Ware, *EPA Urged to Identify, Reduce Barriers To Security of Remote Control Systems*, 36 BNA ENV'T REP. 127 (Jan. 21, 2005) ("When SCADA systems were developed, beginning in the 1960's, few utilities paid attention to security concerns. . .").

145. ASSET BASED VULNERABILITY CHECKLIST, *supra* note 118, at 24 ("Security of SCADA or process control systems are dependent upon several variables including the type of communications used to link Remote Terminal Units (RTUs) to the central terminal unit (e.g. dedicated line, dial-up, fiber, radio frequency, web based, WAN, etc.), access to RTUs and central station, system power supply, and other physical attributes of local IT systems").

146. *See Hearing on Creating the Homeland Security Department*, *supra* note 41, at 196 (statement of Samuel G. Varnado).

147. Ware, *supra* note 144, at 127.

148. EARLY WARNING MONITORING, *supra* note 32, at 8; *see also* Barkham *supra* note 134, at 68 (explaining that the danger of cyber-based attacks increases the more an entity becomes reliant on computerized technology.).

149. *Hearing on Terrorism: Are America's Water Resources and Environment at* Risk, *supra* note 36, at 51 (statement of Ronald L. Dick).

150. De Young & Gravley, *supra* note 25, at 147.

151. Copeland & Cody, *supra* note 3, at 1.

life, property damage, and environmental damage.[152] For example, explosives can destroy pumps, cause large leaks in reservoirs or dam failures, interrupt the electric power supply to facilities, and generally disrupt parts of the water delivery system.[153] This vulnerability is magnified by the fact that "[w]ater system components are extensively interconnected, so destruction of one component may cause a cascading effect."[154]

Furthermore, conventional attacks targeting the storage tanks that house chemicals used to treat and disinfect drinking water supplies, such as chlorine, have the potential to cause deadly consequences. As explained:

> Physical attacks could include the destruction or release of chlorine and other hazardous chemicals used for water treatment. The release of chlorine gas could be deadly within the immediate area of the treatment facility, but the interruption or alteration in the supply of chemicals to the treatment plant preventing disinfection might have more widespread impacts.[155]

Consequently, the most traditional weapons still present a significant threat to drinking water infrastructure security.[156]

F. *Other Drinking Water Security Threats:*

Drinking water facilities depend upon other critical infrastructure sectors, such as the electrical power industry, to operate.[157] Drinking water security may therefore be indirectly threatened by interfering with these other "interconnected" or "interdependent" critical infrastructure elements.[158] As explained:

---

152. De Young & Gravley, *supra* note 25, at 147.

153. EARLY WARNING MONITORING, *supra* note 32, at 8.

154. OFFICE OF RESEARCH AND DEV., U.S. ENV'T PROT. AGENCY, THE WATER SECURITY RESEARCH AND TECHNICAL SUPPORT ACTION PLAN 13 (2004), *available at* http://www.epa.gov/safewater/watersecurity/pubs/action_plan_final.pdf [hereinafter WATER SECURITY RESEARCH AND TECHNICAL SUPPORT ACTION PLAN].

155. De Young & Gravley, *supra* note 25, at 147; *see also* Chilakamarri, *supra* note 18, at 927 (". . .[a] strike on a chlorine disinfectant tank alone, for example, could result in the release of an airborne toxic chlorine cloud which. . .could prove fatal for a widespread population").

156. NAT'L STRATEGY FOR HOMELAND SECURITY, *supra* note 50, at 9 ("Terrorists. . .continue to use traditional methods of violence and destruction to inflict harm and spread fear").

157. *See Hearing on Terrorism: Are America's Water Resources and Environment at* Risk, *supra* note 36, at 51 (statement of Ronald L. Dick) ("There is a great deal of interdependency between water and other infrastructures, the most important being the electric power sector.").

158. *See* Pamela Najor, *EPA Said To Lack Information To Determine Vulnerability of Water Supply To Terrorism*, 34 BNA ENV'T REP. 2078 (Sept. 19, 2003) (discussing a report by EPA's Inspector General indicating that dependence on other critical

> [n]ational security and the quality of life in the United States rely on the continuous reliable operation of a complex set of critical infrastructures: electric power, oil and gas, transportation, water, communications. . .and others. Today, these systems depend heavily on one another; that interdependency is increasing. Disruptions in any one of them could jeopardize the continued operation of the entire infrastructure system.[159]

Because of this increasing interdependence, "[w]hat previously might have been an isolated failure could cascade into a widespread, crippling, multi-infrastructure disruption today."[160] The blackout that struck the northeastern United States during August of 2003 vividly demonstrated how the effects of a power outage can cascade to effectively cripple drinking water facilities.[161] Thus, at present, drinking water systems are only as reliable as the rest of the critical infrastructure network on which they depend.

III.

IT'S BEEN TRIED BEFORE

"Intentional threats against water supplies have been recorded since the earliest archeological and biblical reports of well poisonings."[162] For thousands of years, infecting or poisoning water supplies has been a commonly used military tactic.[163] Dating back as far as 2400 B.C., evidence indicates that ancient Sumerians, Assyrians, Greeks, and Romans all attempted to divert or poison the water supplies of their enemies.[164] Contaminants such as rye ergot, hellebore (skunk cabbage), and cherry laurel

---

infrastructure sectors is a threat to water supply security); *see also* EARLY WARNING MONITORING, *supra* note 32, at 9 (". . .a single source of electrical power [is] prone to disruption by vandalism, terrorism, or acts of nature . . . .").

159. *Hearing on Creating the Homeland Security Department*, *supra* note 41, at 195 (statement of Samuel G. Varnado); *cf. Hearing on Security at Nuclear Facilities Before the Senate Comm. on Env't and Pub. Works*, 107th Cong. (2002) *available at* 2002 WL 1227410 (statement of Dr. Richard A. Meserve discussing the "redundant and separated systems" nuclear power plants use to ensure safety and reliable operation in the event of an attack.).

160. *See Hearing on Creating the Homeland Security Department*, *supra* note 41, at 195 (statement of Samuel G. Varnado).

161. *See* Gibbs, *supra* note 42, at 39 (describing Cleveland's state of emergency after a power outage halted all four pumping stations that lift water out of Lake Erie for use as drinking water and a sewage discharge from inoperable wastewater treatment plants sent bacteria levels on beaches soaring).

162. EARLY WARNING MONITORING, *supra* note 32, at 8.

163. *See* Kornfeld, *supra* note 2, at 441 ("Over the centuries, water systems have been the target of military and terrorist poisoning attacks.").

164. *See id.* at 444-45.

trees (which contain cyanide) were used.[165] This practice continued through the Middle Ages.[166] In 1346, the Tartar Army catapulted plague infested corpses over the walls of a besieged city and reportedly infected the water supplies.[167]

More recently, American armies have both used and been subjected to such practices. During the Civil War, confederate soldiers attempted to poison ponds used by the Union army as drinking water sources by dumping the carcasses of dead animals into them.[168] Conversely, during the Vietnam War, "the Vietcong used fecally contaminated water to sicken American troops."[169]

During the latter portion of the twentieth century, attempts to contaminate water supplies became less of a military tactic and more of a focus for terrorist organizations. These groups continued to use CBW agents in their plots:

- In 1965, Yasir Arafat's Fatah organization attacked the Israeli national water carrier project that transports water from the Jordan River to southern Israel.[170]
- In 1970, "the Weathermen, a group opposed to American imperialism and the Vietnam War, [allegedly] attempted to obtain biological agents to contaminate the water supply systems of US urban centers."[171]
- In 1972, a group called R.I.S.E., led by two college-aged students at a community college, plotted to contaminate the drinking water supplies of Chicago and other Midwestern cities using typhoid and other biological agents.[172] The group managed to prepare significant amounts of bacteria by exploiting one of the group leader's position as a microbiology research assistant at a local hospital.[173]
- In 1982, a plot to contaminate the water supply of Los Angeles with a biological agent was foiled by police and the FBI.[174]

---

165. *See id.*
166. *See* Linkie, *supra* note 103, at 538 n. 45.
167. *See* Guesnier, *supra* note 72, at 182.
168. *See* Kornfeld, *supra* note 2, at 445.
169. *See id.* at 446.
170. *See id.*
171. *See id.*
172. *See* Tucker & Sands, *supra* note 69, at 49.
173. *See* TOXIC TERROR, *supra* note 11, at 57.
174. *See* Kornfeld, *supra* note 2, at 446.

- In 1984, the Rajneesee cult, attempted to contaminate water supplies in Oregon with raw sewage and dead rodents.[175]
- In 1986, a white supremacist group known as "The Covenant, the Sword, and the Arm of the Lord" sought to contaminate urban water supplies with 30 gallons of potassium cyanide they had acquired.[176]
- In 1987, 19 new recruits to the Philippine Army died when an unknown terrorist group contaminated a drinking water source with pesticide.[177]
- In 1998, a water treatment plant in Neenah, Wisconsin was the target of attempted vandalism. A group of teenagers planned on contaminating filters and igniting enough firecrackers to equal ten sticks of dynamite.[178] This "prank" would have extensively damaged the facility and could have potentially released chlorine or ammonia gas into the surrounding area.[179]
- Finally, in 1999, "a bomb blast in Lusaka, Zambia, destroyed the main water pipeline, cutting off water for the city of Lusaka. . .."[180]

Attacks on water supplies have continued into the twenty-first century. The now infamous Taliban regime is reported to have placed dead animals in the drinking water wells of villages unwilling to accept its rule.[181] In 2001, an Australian man demonstrated the vulnerability of SCADA systems by hacking into a computerized waste management system and causing ". . .millions of litres of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel."[182] In 2002, suspects were arrested in Rome attempting to use tunnels under the U.S. embassy to access its water supplies and contaminate them

175. *See* TOXIC TERROR, *supra* note 11, at 132.

176. *See* Tucker & Sands, *supra* note 69, at 49.

177. *See id.* at 50.

178. *See Drinking Water System Security: Hearings Before the Subcomm. on Gov't Efficiency, Financial Management and Intergovernmental Relations of the House Comm. on Gov't Reform*, 107th Cong. (2002) (Testimony of Janet Cherry), *available at*, http://72.14.203.104/search?q=cache:HGhPy17a81IJ:www.cadmusgroup.com/CherryTestimony.pdf [hereinafter *Oversight Hearings On Drinking Water System Security*].

179. *See id.*

180. *See* Kornfeld, *supra* note 2, at 447.

181. *See* De Young & Gravley, *supra* note 25, at 146; *see also Controlling Bioterror*, *supra* note 19, at 5 (also explaining that "U.S. forces in Afghanistan found diagrams of U.S. Public water utilities . . . .").

182. *See* Brenner & Goodman, *supra* note 135, at 31.

with cyanide.[183] Also in 2002, "federal officials arrested two al-Qaeda suspects in the U.S. who apparently were holding documents detailing how to poison water supplies."[184]

Recent history therefore reveals a systematic pattern indicating terrorists' ability to acquire CBW and their continuing intentions to use such agents to attack water supplies.[185] These incidents are not "science fiction," and they will likely continue.[186]

IV.

WAS ANYONE THINKING ABOUT DRINKING WATER SECURITY BEFORE THE SDWA AMENDMENTS?

A. *Drinking Water Infrastructure Security Before September 11th*

"It is a mistake to treat security as a completely new and unfamiliar mission for drinking water systems. . ."[187] Some states and larger individual drinking water facilities have had established programs for over twenty years to address their physical security against intentional acts designed to disrupt their operations.[188] For example, Texas has been "very proactive. . .in adopting state rules to help protect the security of the State's public drinking water."[189] New York City's largest drinking water systems also "have historically focused" on preventing the intentional disruption of water supplies and "have implemented strong programs to prevent and respond" to such incidents.[190] These "strong programs" are due in part to the fact that vulnerability assessments

183. 148 CONG. REC. H638-03, *H639 (daily ed. Fed. 28, 2002) (statement of Rep. Tauzin).

184. Chilakamarri, *supra* note 18, at 945-46.

185. *See* TOXIC TERROR, *supra* note 11, at 1 (CBW are within the technical reach of terrorist organizations).

186. *See* Kornfeld, *supra* note 2, at 447.

187. *See Oversight Hearings On Drinking Water System Security*, *supra* note 178.

188. *See The Progressive State of Texas: Rules and Training*, ASDWA SECURITY UPDATE (Ass'n of State Drinking Water Adm'rs, Washington, D.C.), Fall 2002, at 5; *see also* Craig Jackson, *NY Works to Assure Security of Its Drinking Water Systems*, ASDWA SECURITY UPDATE (Ass'n of State Drinking Water Adm'rs, Washington, D.C.), Winter 2002, at 3.

189. *The Progressive State of Texas*, *supra* note 188, at 5 (discussing Texas' regulatory requirements for "200 foot restricted area zones around intakes; intruder resistant fences enclosing water treatment plants, storage tanks, and pressure maintenance facilities; locking all hatches; disinfecting all public drinking water (including groundwater supplies); and complete treatment. . .of surface water sources").

190. *See* Jackson, *supra* note 188, at 3.

have been a "required component of water supply emergency plans in New York State since 1990."[191]

Federal agencies also began considering the potential threats to drinking water infrastructure long before September 11th. The FBI has been concerned with the consequences of an attack on our nation's drinking water infrastructure for over fifty years.[192] In addition, EPA's Office of Inspector General began specifically researching the vulnerabilities of SCADA systems in the late 1990's after surveys of water utilities indicated that greater efforts were needed to secure their computer networks.[193]

1. Presidential Decision Directive 63

Critical infrastructure protection became of such national concern in the late 1990's that a comprehensive policy was developed to address these security needs.[194] Issued in May 1998, Presidential Decision Directive 63 ("PDD-63") made it the goal of the United States to take "all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures. . ."[195] PDD-63 designated individual "lead agencies" to coordinate security efforts and act as a liaison to private entities within specific infrastructure sectors.[196] EPA was designated the lead agency for water infrastructure protection.[197]

---

191. *Id.*; *see also* EARLY WARNING MONITORING, *supra* note 32, at 7 (recognizing the benefits of utilizing thorough vulnerability assessments to guide implementation of security measures at drinking water facilities).

192. *Controlling Bioterror*, *supra* note 19, at 1 (statement of Rep. Paul Gillmor).

193. *See* Ware, *supra* note 144, at 127; *see also* EARLY WARNING MONITORING, *supra* note 32, at 8 (discussing that the President's Commission on Critical Infrastructure Security (1997) found that cyber threats against drinking water utilities are a growing concern.).

194. *See* Kornfeld, *supra* note 2, at 459-60 (discussing the legislative background surrounding the establishment of Presidential Decision Directive 63); *see also* EXPERTS' VIEWS ON HOW FEDERAL FUNDING CAN BEST BE SPENT TO IMPROVE SECUIRTY at 5, *reprinted in Controlling Bioterror*, *supra* note 137, at 48.

195. *White Paper, The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63* at 2 (May 22, 1998) *available at* http://www.fas.org/irp/offdocs/paper598.htm.

196. *See id.* at Annex A; *cf. Hearing on Creating the Homeland Security Department*, *supra* note 41, at 196 (discussing that while the "stovepiped approach" of examining the vulnerabilities of individual infrastructure elements is important, "the more compelling problem is to address the interdependent nature of the behavior" of the various infrastructure elements).

197. *See White Paper*, *supra* note 195, at Annex A. For a discussion of other Presidential Decision Directives guiding EPA's pre-September 11th counterterroism and

"Private-public partnerships," such as that between EPA and the drinking water industry, were the primary mechanism for fulfilling PDD-63's directives.[198] A crucial responsibility of these partnerships was to develop sector specific infrastructure protection plans.[199] These individual plans, compiled as part of an overall "National Infrastructure Assurance Plan," included vulnerability assessments of the sector as a whole, strategies for eliminating significant vulnerabilities, and remedial plans to recover from terrorist attacks.[200]

PDD-63 also recognized the rapidly changing universe of critical infrastructure threats, as well as the need for "robustly adaptive" responses to such threats.[201] Consequently, unlike the SDWA Amendments, PDD-63 required periodic updates of the vulnerability assessments based upon emerging threat information so that they would remain current.[202] In order to provide the current threat information needed to facilitate salient vulnerability assessments updates, PDD-63 included information-gathering requirements.[203] The intelligence community was directed to develop and implement a plan for "enhancing collection and analysis of the foreign threat to our national infrastructure. . .."[204] PDD-63 also "strongly encourage[d]" the establishment of Information Sharing and Analysis Centers ("ISACs") to "serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the [FBI]."[205] Accordingly, PDD-63 emphasized

---

preparedness duties, *see generally, Hearing on Response to Bioterrorism By Federal Agencies Before the House Committee on Science*, 107th Cong. (2001) (statement of Linda Fisher, Deputy Administrator, U.S. Env't Prot. Agency), *available at* http://www.house.gov/science/dec05/fisher.htm.

198. *See White Paper*, *supra* note 195, at 2 (discussing that these public-private partnerships sought "to avoid outcomes that increase government regulation or expand unfunded mandates to the private sector").

199. *See id.*

200. *See id.* at 5; *see also* WATER SECURITY RESEARCH AND TECHNICAL SUPPORT ACTION PLAN, *supra* note 154, at 6 (discussing the drinking water sector's responsibilities in contributing to the National Infrastructure Assurance Plan.).

201. *See White Paper*, *supra* note 195, at 3.

202. *See id.* at 5.

203. *See id.* at 3.

204. *See id.* at 5.

205. *See id.* at 8-9 (explaining that such ISACs "would establish baseline statistics and patterns on the various infrastructures, become a clearinghouse for information within and among the various sectors, and provide a library for historical data to be used by the private sector . . . .").

the need for incorporating up-to-date threat intelligence into infrastructure security planning.

Ultimately, PDD-63 did not reach its full potential because its original intent of addressing a broad range of infrastructure threats was never fulfilled.[206] In 2003, President Bush partially superseded PDD-63 by issuing Homeland Security Presidential Directive 7 ("HSPD-7").[207] Nevertheless, HSPD-7 maintains EPA's role as the lead agency in change of drinking water infrastructure security, as well as many of the same infrastructure security goals established by PDD-63.[208] Thus, despite its shortcomings, PDD-63 serves as a blueprint for current infrastructure protection requirements.[209]

2. Other Past Efforts Benefiting Drinking Water Security

Drinking water infrastructure security also has benefited indirectly from the steadily increasing attention given to understanding and preparing for terrorist threats, especially bioterrorism.[210] Many initiatives started in the 1990's helped develop responses still relevant to addressing the consequences of bioterror attacks on various targets, including drinking water facilities.[211] Prior in-

206. EXPERTS' VIEWS ON HOW FEDERAL FUNDING CAN BEST BE SPENT TO IMPROVE SECUIRTY, at 5, *reprinted in Controlling* Bioterror, *supra* note 137, at 48 (explaining that much of the effort undertaken by the public-private partnerships focused narrowly on cyber-security issues.).

207. *See* Press Release, Office of the Press Secretary, White House, Homeland Security Presidential Directive/HSPD-7: Subject: Critical Infrastructure Identification, Prioritization, and Protection at ¶ 37 (December 17, 2003) *available at* http://www.fas.org/irp/offdocs/nspd/hspd-7.html (expressly superseding PDD-63 to the extent of any inconsistencies between the two directives).

208. *See id.* at ¶ 18(c).

209. *See* De Young & Gravley, *supra* note 25, at 149 ("Initial water supply protection steps by the Bush administration appear to build upon, rather than replace or duplicate. . ." the structure of PDD-63.).

210. *See* Hodge, *supra* note 105, at 254 ("Prior to September 11, federal and state public health authorities had already allocated some resources and engaged in efforts to prevent a major bioterrorism event."); *see also* Sokolski, *supra* note 98, at 207 ("Well before . . . 1995, the Defense Department was forced to consider the implications of a biological weapons attack . . . ."); Gene W. Matthews et al., *Legal Preparedness for Bioterrorism*, 30 J.L. MED. & ETHICS 52 (2002) ("The CDC has been concerned with and focused on bioterrorism preparedness for several years – well in advance of the events of September and October 2001.").

211. *See* Bacevich, *supra* note 74, at 222 (noting the several hundred million dollars being spent by federal agencies to stockpile antibiotics and train emergency response teams); *see also* Sokolski, *supra* note 98, at 208 (discussing the intention to spend $10 billion in fiscal year 2000 on countering terrorism, including biological and chemical threats, and the creation of National Guard response units (formerly known as Rapid Assessment and Initial Detection ("RAID") teams, now known as

ternational and domestic legislative efforts also were taken to stop the proliferation of biological and chemical weapons.[212] Such legislation has helped prevent biological and chemical weapons from becoming available to would-be attackers. However, these prior efforts at planning for domestic terrorism were criticized for the "absence of strong leadership and a failure to achieve a crosscutting, coordinated program with identified resources in the federal budget."[213] Consequently, even before September 11th, some had called for a comprehensive bioterrorism statute with strikingly similarities to the Public Health Security and Bioterrorism Preparedness and Response Act of 2002.[214]

B. *Criticisms of Prior Drinking Water Security Practices*

Prior efforts to protect the nation's drinking water infrastructure have been criticized as inadequate given the renewed concern over modern post-September 11th terrorist threats.[215] Critics argue that "until the 1990's emergency planning at drinking water facilities *generally* focused on responding to natural disasters, and in some cases, domestic threats such as vandalism."[216] Terrorism involving the intentional contamination of water and wastewater systems did not receive much attention by facility operators as a viable national security threat

---

Civil Support Teams (CSTs) to help local authorities respond to chemical and biological attacks).

212. *See generally* Fidler, *supra* note 101, at 8-9 (discussing the Biological Weapons Convention of 1972 and the Chemical Weapons Convention of 1993); *see also* Heather A. Dagen, *Bioterrorism: Perfectly Legal*, 49 CATH. U. L. REV. 535 (2000).

213. Victoria V. Sutton, *A Precarious "Hot Zone" - The President's Plan to Combat Bioterrorism*, 164 MIL. L. REV. 135, 151 (2000) (explaining that the various departments and agencies "did not fully understand the scope of the problem they were purporting to address.").

214. *See id.* at 152 ("There is an immediate need to propose a statute, with a title such as the Bioterrorism Research, Preparedness and Responsiveness Program. . ."); *see also* Public Health Security and Bioterrorism Preparedness and Response Act of 2002, Pub. L. No. 107-188, 116 Stat. 594, (2002).

215. *See* Ron Booth et al., *Securing Water Utilities: Beyond Vulnerability Assessments*, OPFLOW (Am. Water Works Assoc., Denver, Co.), June 2004, at 1 (". . .securing water infrastructure. . .cannot be properly accomplished with old methods").

216. EXPERTS' VIEWS ON HOW FEDERAL FUNDING CAN BEST BE SPENT TO IMPROVE SECUIRTY, at 5, *reprinted in Controlling* Bioterror, *supra* note 137, at 48 (emphasis added); *see also* PROTECTING OUR WATER, *supra* note 12, at 9 (explaining that "most traditional emergency response plans are developed to respond to a natural event, such as a hurricane, tornado, or earthquake, or an event such as a major water main break").

before September 11th.[217] While isolated examples to the contrary exist, most drinking water facilities therefore did not consider such terrorist threats in their prior vulnerability assessments and emergency planning programs. Thus, critics of historical drinking water security efforts claim that they are insufficient to address today's "serious terrorist threats."[218]

The prior lack of concern regarding terrorist threats to drinking water infrastructure security is often manifested in facilities' historical design and use. Drinking water facilities constructed "prior to World War II were built to be visible and accessible. . .."[219] They were "public building[s], usually built close to the center of town" and oftentimes used as a visitor's center.[220] The security measures used by such facilities since the late 1940s, such as perimeter fencing, intrusion detection devices, closed-circuit television, and personnel-entry control, were not intended to prevent post-September 11th type threats.[221]

However, these criticisms may be unwarranted. By the 1990's, both government and industry officials "broadened the process" of evaluating drinking water infrastructure security "to account for terrorist threats."[222] Furthermore, "the types and extent of contamination and the health effects resulting from physical acts of terrorism are often – but not always – similar to the consequences of traditional system contamination that concern water system managers every day."[223] Consequently, while some aspects of the threats currently facing drinking water systems are new, "the framework in which they should be considered is familiar to water system managers and operators as well as state regulatory agencies and the U.S. EPA."[224]

While September 11th "served as a springboard for radical and far-reaching legislation intended to enable countries to better detect, prevent, prosecute, and ultimately, put an end to terrorism,"

---

217. *See* Kornfeld, *supra* note 2, at 439; *see also* Chilakamarri, *supra* note 18, at 927.

218. *See* Copeland & Cody, *supra* note 3, at 3.

219. Booth et al., *supra* note 215, at 4.

220. *Id.*

221. *See id.* (security systems were installed to facilitate prosecutions of trespassers and "to prevent lawsuits by people injuring themselves on utility property").

222. EXPERTS' VIEWS ON HOW FEDERAL FUNDING CAN BEST BE SPENT TO IMPROVE SECUIRTY, at 5, *reprinted in Controlling Bioterror*, *supra* note 137, at 48.

223. *See Oversight Hearings On Drinking Water System Security*, *supra* note 178 (explaining that "[t]he public health tradition already accommodates the kinds of analysis, planning, and response necessary to counter a deliberate attack").

224. *See id.*

it is not this country's starting point for addressing drinking water infrastructure security.[225] However, it is undeniable that regardless of how effective the first steps were, "[e]fforts to better protect drinking water infrastructure were accelerated dramatically after the September 11 attacks."[226] "Unfortunately, it took the scare our Nation felt. . .[on September 11th] before Congress took action to fill in the legal gaps that prevented real preparedness from occurring."[227]

V.

THE CURRENT LEGAL RESPONSE TO SECURING DRINKING WATER INFRASTRUCTURE: THE DRINKING WATER SECURITY AND SAFETY AMENDMENTS OF THE PUBLIC HEALTH SECURITY AND BIOTERRORISM PREPAREDNESS AND RESPONSE ACT OF 2002

On June 12, 2002, new security requirements for all community water systems serving more than 3,300 people were mandated when President Bush signed into law the SDWA Amendments.[228] These approximately 8,000 utilities serve over 240 million people, or about 90 percent of the nation's population served by community water systems.[229] The SDWA Amendments' requirements focus on preventing terrorist and other intentional acts intended to "substantially disrupt the ability of [drinking water systems] to provide a safe and reliable supply of drinking water."[230] This focus on terrorist or other intentional acts was intended to "[stand] apart" from the common historical

225. Joshua D. Zelman, *Recent Developments in International Law: Anti-Terrorism Legislation-Part One: An Overview*, 11 J. TRANSNAT'L L. & POL'Y 183 (2001); *see also* Press Release, *supra* note 5, at 2 (explaining that after PDD 63 was established, the lead private sector drinking water agency "began to prepare technical materials and publications for water utilities relating to water system security").

226. *Controlling Bioterror*, *supra* note 19, at 48 (statement of John B. Stephenson).

227. *Id.* at 1; *see also Interview With Matthew Meselson, Professor of Molecular and Cellular Biology, Harvard University*, 6 GEO. PUB. POL'Y REV. 107, 110 (2001) ("People don't get concerned with something until it happens.") [hereinafter *Meselson*].

228. *See* 42 U.S.C. § 300f(1) (2006) (defining a "community water system" as a public drinking water system that "serves at least 15 service connections used by year-round residents of the area served by the system" or "regularly serves at least 25 year-round residents"); *see also* Public Health Security and Bioterrorism Preparedness and Response Act of 2002, *supra* note 6.

229. PROTECTING OUR WATER, *supra* note 12, at 5.

230. 42 U.S.C. § 300i-2(a)(1) (2006); *see also* PROTECTING OUR WATER, *supra* note 12, at 5 (explaining that the focus of the SDWA Amendments is purposeful destruction or contamination of water supplies).

infrastructure security concerns of drinking water facilities, such as natural disasters and vandalism.[231]

A. *SDWA Amendment Provisions*

Under the SDWA Amendments, drinking water facilities are required to:

- Conduct a vulnerability assessment of their major system components;[232]
- Certify that the vulnerability assessment complies with the requirements of SDWA § 300i-2(a)(1) and submit a copy of it to EPA by the statutory deadlines;[233]
- Prepare or revise an emergency response plan that incorporates the results of the vulnerability assessment and identifies the resources and means necessary to address the identified security issues; and[234]
- Certify to EPA, within 6 months of completing the vulnerability assessment, that the drinking water system has completed or updated their emergency response plan.[235]

The SDWA Amendments also authorize grant money to assist community water systems in meeting the SDWA Amendments' requirements, direct that research be conducted regarding potential drinking water threats and methods to address them, and increase the penalties for intentionally contaminating or threatening to contaminate regulated community water supplies.

1. Vulnerability Assessments and Emergency Response Plans:

Vulnerability assessments and emergency response plans are the cornerstone requirements of the SDWA Amendments.[236] These documents are integral planning tools for addressing drinking water security issues both at individual facilities and

231. *See* PROTECTING OUR WATER, *supra* note 12, at 6; *cf. supra* Section IV(B).

232. *See* EPA, *Requirements of the Public Health and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act)*, *at* http://www.epa.gov/safewater/security/bioterrorism.cfm; *see also* U.S. ENVT'L PROT. AGENCY, OFFICE OF WATER, INSTRUCTIONS TO ASSIST COMMUNITY WATER SYSTEMS IN COMPLYING WITH THE PUBLIC HEALTH SECURITY AND BIOTERRORISM PREPAREDNESS AND RESPONSE ACT OF 2002 4 (Jan. 2003) [hereinafter INSTRUCTIONS TO ASSIST COMMUNITY WATER SYSTEMS].

233. *See* INSTRUCTIONS TO ASSIST COMMUNITY WATER SYSTEMS, *supra* note 232.

234. *See id.*

235. *See id.*

236. *See* 42 U.S.C. § 300i-2(a)(1) (2006).

across the entire infrastructure sector.[237] Together, they help achieve the SDWA Amendments' goals of safeguarding public health and reducing the potential for disruption of the country's supply of safe drinking water.[238]

a. Vulnerability Assessments

Vulnerability assessments serve multiple critical purposes. A vulnerability assessment is a "systematic analysis" of a drinking water facility's components that evaluates their susceptibility to potential threats.[239] Such analyses help drinking water facility operators ". . .identify key locations that are vulnerable to intentional contamination. . ."[240] Community water systems have the flexibility "to utilize any methodology or tool" for conducting vulnerability assessments as long as all of the following system components and operations are reviewed:

1) Pipes and constructed conveyances;
2) Physical barriers;
3) Collection; pretreatment; and treatment, storage, and distribution systems;
4) Electronic, computer, or automated systems;
5) Use, storage, and handling of chemicals;
6) System operation and maintenance.[241]

EPA was explicitly "not given any rulemaking or other authority" to establish further requirements for what is or is not an acceptable vulnerability assessments.[242] Nevertheless, EPA has issued guidance regarding factors drinking water facilities should

---

237. *See* NAT'L STRATEGY FOR HOMELAND SECURITY, *supra* note 50, at 17 ("Vulnerability assessments. . .allow planners to project the consequences of possible terrorist attacks against specific facilities or different sectors of the economy or government. These projections allow authorities to strengthen defenses against different threats").

238. *See* U. S. ENVT'L PROT. AGENCY, VULNERABILITY ASSESSMENT FACTSHEET, *available at* http://www.epa.gov/watersecurity/pubs/va_fact_sheet_12-19.pdf.

239. *See* EPA, *Large Drinking Water Utilities Awarded Water Security Grants* 3 (July 21, 2003), *at* http://www.epa.gov/watersecurity/pubs/va_fact_sheet_12-19.pdf (on file with author); *see also* VULNERABILITY ASSESSMENT FACTSHEET, *supra* note 238.

240. RESPONSE PROTOCOL TOOLBOX, MODULE 1, *supra* note 36, at 22.

241. *See* U.S. ENVT'L PROT. AGENCY, OFFICE OF WATER, ADDENDUM TO THE INSTRUCTIONS TO ASSIST COMMUNITY WATER SYSTEMS IN COMPLYING WITH THE PUBLIC HEALTH SECURITY AND BIOTERRORISM PREPAREDNESS AND RESPONSE ACT OF 2002 5 (Oct. 2003); *see also* 42 U.S.C. § 300i-2(a)(1) (2006).

242. *See* 147 Cong. Rec. E2410 (Dec. 20, 2001) (statement of Rep. Gillmor).

consider in evaluating these components as they prepare their vulnerability assessments.[243]

Awareness and understanding of a drinking water facility's vulnerabilities is critically important because it ". . .provide[s] a basis for improving physical security against intentional contamination and preparing for the evaluation of contamination threats."[244] In other words, "[t]he more we know about our vulnerability, the better able we are to protect ourselves."[245] Effective vulnerability assessments serve "as a guide to the water utility by providing a prioritized plan for security upgrades, modifications of operational procedures, and/or policy changes to mitigate the risks and vulnerabilities to the utility's critical assets."[246] Furthermore, by identifying potential security concerns, vulnerability assessments provide a framework for prioritizing the "long-term investment of effort and resources" in developing such "risk reduction options."[247] Aggregated information derived from vulnerability assessments may also be used as a basis for making broader sector-wide funding allocation decisions.[248]

Vulnerability assessments are not only useful as planning tools. They also provide the foundation for emergency response actions.[249] Vulnerability assessments are a "potential source of information to consider" when evaluating the credibility of threatened or actual contamination events and in deciding whether response actions are warranted.[250] The information contained in vulnerability assessments allows drinking water facility operators to evaluate whether a contamination event is likely to affect locations that are high-value targets of contamination or particularly vulnerable to the intentional introduction of con-

243. *See generally* VULNERABILITY ASSESSMENT FACTSHEET, *supra* note 238 (discussing in detail the factors to be considered for each vulnerability assessment element).

244. RESPONSE PROTOCOL TOOLBOX, MODULE 1, *supra* note 36, at 22.

245. NAT'L STRATEGY FOR HOMELAND SECURITY, *supra* note 50, at 7.

246. VULNERABILITY ASSESSMENT FACTSHEET, *supra* note 238 (from the vulnerability assessments, drinking water facilities may "identify corrective actions that can reduce or mitigate the risk of serious consequences from adversarial actions (e.g., vandalism, insider sabotage, terrorist attack, etc.).").

247. NAT'L STRATEGY FOR HOMELAND SECURITY, *supra* note 50, at 33; *see also* VULNERABILITY ASSESSMENT FACTSHEET, *supra* note 238.

248. *Controlling Bioterror*, *supra* note 19, at 45 (statement of John B. Stephenson).

249. *See* Harris, *supra* note 15, at 2, *reprinted in Controlling Bioterror*, *supra* note 15, at 2.

250. RESPONSE PROTOCOL TOOLBOX, MODULE 2, *supra* note 60, at 26-27.

taminants.[251] This information helps drinking water facility operators determine whether the need for response actions, such as shutting down the outflow of affected water, public notification of potential contamination, and providing alternate water supplies, has been triggered. Accordingly, vulnerability assessments are invaluable tools, both from risk management and response perspectives.

b. ERPs

The SDWA Amendments also require that drinking water facilities prepare or revise an Emergency Response Plan ("ERP") "that incorporates the results" of their vulnerability assessment.[252] ERPs serve as ". . .a guide for water utilities upon which actions and decisions can be based to govern the immediate response to an emergency."[253] ERPs are required to include ". . .plans, procedures, and identification of equipment that can be implemented or utilized in the event of a terrorist or other intentional attack on the public water system."[254] They are intended ". . .to identify certain responsibilities delegated to various teams and employees, present details of the notification procedures, and describe alternate measures and response actions."[255] In addition to the facility employees, "[t]he community's public health and law enforcement officials, emergency responders, laboratories, and technical assistance providers and all their roles in emergency response are identified in the ERP."[256] As with vulnerability assessments, ERPs are required

251. *See id.* at 27 (Vulnerability assessments are "of particular value during the evaluation of general contamination threats in which neither a location nor a contaminant is specified or suspected.").

252. *See* 42 U.S.C. § 300i-2(b) (2006).

253. *Large Drinking Water Utilities Awarded Water Security Grants*, *supra* note 239, at 3.

254. 42 U.S.C. § 300i-2(b) (2006) (ERPs are also to include "actions, procedures, and identification of equipment which can obviate or significantly lessen the impact of terrorist attacks or other intentional actions on the public health and safety and supply of drinking water provided to communities and individuals.").

255. *Large Drinking Water Utilities Awarded Water Security Grants*, *supra* note 239, at 3.

256. John Stubbart, *How Do We Correlate Our Paperwork*, OPFLOW (Am. Water Works Ass'n., Denver, Co.), May 2005, at 11; *see also* 42 U.S.C. § 300i-2(b) (2006) (requiring that community water systems prepare or revise their ERPs in coordination ". . .with existing Local Emergency Planning Committees established under the Emergency Planning and Community Right-to-Know Act (42 U.S.C. § 11001 et seq.)" – usually meaning the local fire department).

to focus on terrorist or other intentional acts.[257]

However, drinking water facilities are not required to submit the actual ERP to EPA. Utilities need only certify to EPA that they have completed the ERP within six months of completing their vulnerability assessment.[258]

2. EPA's Regulatory and Enforcement Authority Under the SDWA Amendments

Several SDWA provisions authorize EPA to enforce the requirements of the SDWA Amendments and take action against incidents involving the intentional contamination of drinking water facilities.[259] First, SDWA § 300g-3 "gives the EPA general authority to issue administrative orders or pursue injunctive or other civil relief" for violating "applicable requirements" under the SDWA Amendments, such as the certification requirements under section 1433(a)(2) and 1433(b).[260] Drinking water facilities face significant penalties under this provision for failing to submit vulnerability assessments or ERPs certifications before the statutory deadlines, or for submitting false information in vulnerability assessments and ERPs certifications.[261] Offenses involving the submission of false or misleading information may also lead to criminal penalties under other statutes.[262]

The SDWA Amendments also substantially increased criminal and civil penalties under SDWA § 300i-1 for "tampering offenses."[263] Tampering offenses are defined as the actual, attempted, or threatened introduction of "a contaminant into a public water system with the intention of harming persons" or "otherwise interfer[ing] with the operation of a public water sys-

257. PROTECTING OUR WATER, *supra* note 12, at 8 (explaining that this focus is ". . .in distinction to plans that most utilities have had for years dealing with natural disasters. . ." or emergencies such as water main breaks).

258. *See* 42 U.S.C. § 300i-2(b) (2006).

259. *See generally* Chilakamarri, *supra* note 18, at 929.

260. *See id.*; *see also* Pub. L. No. 107-188, *supra* note 7, at § 403(1), 116 Stat. 594, 687 (including vulnerability assessments and ERPs as "applicable requirements" under SDWA § 300g-3(i)(I)).

261. *See Instructions to Assist Community Water Systems in Complying*, *supra* note 232, at 6.

262. *See* 18 U.S.C. § 1001 (2006) (providing criminal penalties for knowingly submitting false or fraudulent information in "in any matter within the jurisdiction" of the executive branch of the U.S. government).

263. *See, e.g.*, 42 U.S.C. § 300i-1(a) (2006) (increasing the maximum prison sentence for tampering offenses from five to 20 years); *see also* 42 U.S.C. § 300i-1(c) (2006) (increasing the maximum civil penalties for tampering offenses from $50,000 to $1,000,000).

tem with the intention of harming persons."[264] The increased penalties for these offenses were intended to provide a strong deterrent against would-be attacks on public drinking water supplies.

Lastly, SDWA § 300i provides EPA with emergency powers to pursue administrative or civil actions for monetary and injunctive relief "in cases where there may be an imminent and substantial endangerment to public health" due to the actual or threatened contamination of a community water system.[265] The SDWA Amendments expanded the type of incidents constituting an "imminent and substantial endangerment to health" to include "a threatened or potential terrorist attack (or other intentional act designed to disrupt the provision of safe drinking water or to impact adversely the safety of drinking water supplied to communities and individuals)..."[266] EPA's expanded authority under this provision allows it to act even when there is only a threatened incident and "no actual 'contamination' of a water supply."[267]

The SDWA's existing enforcement framework was largely unchanged by the SDWA Amendments. Penalties for existing tampering offenses were simply increased and EPA's ability to bring imminent and substantial endangerment actions based on threatened or actual terrorist attacks was only narrowly augmented.[268] Most importantly, EPA was explicitly not granted any authority to impose or enforce additional regulatory requirements upon drinking water facilities beyond those specified in the SDWA Amendments.[269] Consequently, whether EPA was granted sufficient regulatory and enforcement authority to ensure that drinking water facilities effectively address known security vulnerabilities and achieve the SDWA Amendments' overarching goal is greatly disputed among Congress, the regulated community, and EPA itself.[270]

3. Research Requirements

The SDWA Amendments also require EPA to collaborate with other appropriate governmental entities in reviewing the state of

264. 42 U.S.C. § 300i-1(d) (2006).
265. *See* Chilakamarri, *supra* note 18, at 929.
266. 42 U.S.C. § 300i-1(a) (2006).
267. *See* Chilakamarri, *supra* note 18, at 932.
268. *See generally id.* at 927 (discussing EPA's narrow authority to bring imminent and substantial endangerment actions under the SDWA Amendments).
269. *See* 147 Cong. Rec. E2410, *supra* note 242 (statement of Rep. Gillmor).
270. *See generally Controlling Bioterror*, *supra* note 19, at 1.

knowledge regarding various threats to drinking water infrastructure security, as well as the methods for addressing such threats. Section 1435 of the SDWA Amendments requires EPA to review methods by which drinking water systems ". . .and all its parts could be intentionally disrupted or rendered ineffective or unsafe, including methods to interrupt the physical infrastructure, the computer infrastructure, and the treatment process."[271] Section 1434 of the SDWA Amendments requires EPA to review "current and future methods to prevent, detect, and respond" to the intentional contamination of community water systems and their source waters.[272] EPA is specifically directed to

> . . .review methods for detecting contamination levels, preventing the flow of contaminated water to the public, negating or mitigating the health effects of contamination, providing notice to CWS users and operators if contamination occurs, developing education programs for CWSs, and reviewing biomedical research on health effect of various contaminants.[273]

Research into early warning notification and real-time monitoring systems, as well as innovative drinking water treatment methods, are priorities under these provisions.[274]

EPA is directed to disseminate the information it develops under these sections, as deemed appropriate, through the Information Sharing and Analysis Center ("ISAC") or other appropriate means.[275] However, there is no requirement under the SDWA Amendments that either vulnerability assessments or ERPs ever be updated to reflect this new information as it becomes available.

VI.
ARE THE SDWA AMENDMENTS NECESSARY TO PROTECT OUR DRINKING WATER?

The SDWA Amendments' relevance to protecting public health depends primarily upon the likelihood a potential attacker could successfully contaminate or disrupt drinking water infra-

271. *Id.* at 42; *see also* 42 U.S.C. § 300i-4(a) (2006).

272. *See* 42 U.S.C. § 300i-3(a) (2006); *see also* Chilakamarri, *supra* note 18, at 931.

273. *See* Chilakamarri, *supra* note 18, at 931; *see also Controlling Bioterror*, *supra* note 19, at 42.

274. *See* 42 U.S.C. § 300i-3(a)(1) (2006).

275. *See* 42 U.S.C. § 300i-4(d) (2006).

structure systems.[276] The SDWA Amendments' value also depends upon whether other existing environmental laws already impose similar security requirements for drinking water facilities. Given the drinking water industry's "virtually unprecedented" mobilization of effort and resources to comply with the SDWA Amendments, it is important to ensure that the new requirements will yield meaningful and distinct improvements to drinking water infrastructure security.[277] Otherwise, the SDWA Amendments' requirements add nothing more than an expensive duplicate layer of regulation that can actually be counterproductive to the SDWA Amendments' goals.[278] This section examines both the likelihood of the threats facing drinking water infrastructure, as well as the similarity of competing security requirements under other existing environmental laws.

A. *Is Drinking Water Infrastructure Facing a Likely Threat?*

There is widespread consensus that "[a]ll drinking water plants are, to some degree, vulnerable to intentional contamination incidents" and disruption of service attacks.[279] It is simply ". . .unreasonable to expect that every part of the infrastructure can be completely protected."[280] However, policy choices and legislative action cannot be based solely upon the virtually infinite vulnerability of our critical drinking water infrastructure and the potential consequences of a successful attack.[281] Bluntly stating that "[w]e're under attack; that's the way it is" is insufficient.[282]

276. *See* RESPONSE PROTOCOL TOOLBOX, MODULE 2, *supra* note 62, at 15 ("The primary focus of the threat evaluation is public health (i.e., has the water been contaminated at levels of public health concern).").

277. *See* PROTECTING OUR WATER, *supra* note 12, at 3; *see also* NAT'L STRATEGY FOR HOMELAND SECURITY, *supra* note50, at 63-64 (resources should only be allocated for homeland security activities "where the benefit of reducing risk is worth the amount of additional cost").

278. *See* Sokolski, *supra* note 98, at 210 (discussing the risks of overestimating the threat of domestic biological and chemical terrorism).

279. *See* RESPONSE PROTOCOL TOOLBOX, MODULE 1, *supra* note 36, at 22; *see also* EARLY WARNING MONITORING, *supra* note 32, at 5.

280. *Hearing on Creating the Homeland Security Department*, *supra* note 41, at 196 (statement of Samuel G. Varnado); *see also* Barry Kellman, *An International Criminal Law Approach to Bioterrorism*, 25 HARV. J. L. & PUB. POL'Y 721, 722 (2002) ("The United States is starkly vulnerable to a terrorist attack involving pathogens. . .").

281. *See* TOXIC TERROR, *supra* note 11, at 1; *see also* Matthews et al., *supra* note 210, at 53-54 ("Times of fear and terror have often, if not always, led to what hindsight teaches were unnecessary and ineffective deprivations of individual rights. . .").

282. Remarks at a meeting of the President's Homeland Security Advisory Council, 38 WEEKLY COMP. PRES. DOC. 1000 (June 17, 2002).

The actual likelihood of the threat facing drinking water infrastructure must first be carefully assessed.[283]

If the threat of attack on drinking water supplies is generally implausible, the "nearly infinite" vulnerability and potentially catastrophic consequences become increasingly irrelevant.[284] For example, we may all be highly vulnerable to an asteroid colliding with the Earth, and the consequences of such an event could destroy the planet. However, the actual likelihood of such a threat is considered remote. Consequently, massive efforts to address such an unlikely threat are generally considered unnecessary.

Similarly, requiring drinking water facilities to implement billions of dollars in security measures to prevent unlikely threats is unnecessary and wasteful.[285] Limited resources are further squandered when drinking water facilities' response action protocols are repeatedly triggered by unlikely threats. Because of the public's sensitivity to even the "mere threat" of contaminated drinking water, such "false alarms" could ". . .result in undue panic and stress on the public," and may severely impact citizens' day-to-day life by making otherwise safe water unavailable.[286] Thus, overemphasizing unlikely drinking water threats risks diluting the focus of security efforts away from likely threats, and erodes the underlying purpose of the SDWA Amendments – assuring the public of a "safe and reliable supply of drinking water."[287] Accordingly, the competing views on whether drinking water infrastructure faces a likely threat from terrorist attack must be examined.

283. TOXIC TERROR, *supra* note 11, at 1.

284. NAT'L STRATEGY FOR HOMELAND SECURITY, *supra* note 50, at 3.

285. *See* PROTECTING OUR WATER, *supra* note 12, at 14 (estimating the national cost of implementing improved basic security measures at drinking water facilities at $1.6 billion).

286. RESPONSE PROTOCOL TOOLBOX, MODULE 2, *supra* note 62, at 10; *see also id.* at 17 (discussing impacts of response actions on consumers), *id.* at 44 (". . .[C]onsumers may be instructed to boil water, limit their water uses to activities that do not involve consumption, or not use the water at all. . .[Such response actions] will have a significant impact on consumers"); *see also* RESPONSE PROTOCOL TOOLBOX, MODULE 1, *supra* note 36, at 19.

287. *See* Dagen, *supra* note 212, at 537 (". . .continually having to respond to these threats may eventually desensitize people to the possibility of actual attacks"); *see also* 42 U.S.C. § 300i-2(a)(1).

1. There are many viable threats to drinking water security

a. NBC, Conventional, and Cyber-Based Attacks

The prevailing view among experts is that conventional, as well as radiological, biological, and chemical ("NBC") weapons all represent viable threats to drinking water infrastructure security.[288] ". . .[I]t is possible to contaminate a portion of a drinking water system, resulting in adverse public health consequences."[289] In addition, the threat posed to drinking water infrastructure components from cyber-based attacks is a top concern. Despite the various technical challenges involved in successfully using such weapons to attack drinking water supplies, they continue to be the key threats that all "[a]ctive and effective security programs should consider. . ."[290] Accordingly, the SDWA Amendments' goal of securing drinking water facilities against these threats is well-founded.

i. Conventional Weapons

Conventional explosives are perhaps the likeliest threat to drinking water infrastructure.[291] A well-placed bomb at a major treatment facility, pumping station, or water intake could deprive large areas of a city of drinking water for months.[292] Materials for making explosives are readily available.[293] Unlike biological, chemical, or radiological weapons, there are far fewer technical hurdles to manufacturing explosives, and their use has a "relatively high chance for successful execution."[294] Accordingly, explosives are still the weapon of choice for terrorist organizations across the world. Sadly, there are virtually daily demonstrations

288. *See, e.g.,* Habib, *supra* note 44, at 5; *see also* Najor, *supra* note 158, at 2078-79 (discussing an EPA Inspector General report which noted that "potential threats to the nation's water supply include contamination with biological, chemical, or radiological agents, or destruction of physical infrastructure).

289. RESPONSE PROTOCOL TOOLBOX, MODULE 2, *supra* note 62, at 10; *see also* Dagen, *supra* note 212, at 535 ("The possibility of a large-scale biological weapons attack occurring within the United States is more than merely hypothetical").

290. *See* WATER SECURITY WORKING GROUP FINDINGS, *supra* note 30, at vii.

291. *See* De Young & Gravley, *supra* note 25, at 147 (". . .[P]hysical attacks on water system components pose a more likely and therefore more significant threat to public water supplies."); *see also* EARLY WARNING MONITORING, *supra* note 32, at 8.

292. *See* EARLY WARNING MONITORING, *supra* note 32, at 9 ("The destruction of motors or pumps at major pumping stations is disastrous because repairs may take months").

293. *See* NAT'L STRATEGY FOR HOMELAND SECURITY, *supra* note 50, at 9.

294. *Id.*

of this preference.[295] Conventional weapons therefore pose a likely threat to critical drinking water infrastructure.[296]

ii. Cyber-Based Attacks

Cyber-based attacks on SCADA systems are another likely threat to drinking water infrastructure security.[297] "[I]t is possible to covertly and easily take over control of. . .[SCADA] systems and cause disruptions with significant consequences."[298] While some believe that hacking into a SCADA system ". . .would be a lot harder than learning to fly an airplane. . .," terrorists have demonstrated their dedication to achieving their violent objectives.[299] Terrorists are known to be both well-versed in computers and "internet savvy."[300]

Using cyberspace to carry out attacks on drinking water infrastructure offers terrorists many of the advantages of using conventional weapons; "[a]ccess to cyberspace is even easier to obtain than conventional explosives."[301] "A terrorist mounting a cyberterror attack runs no risk of contamination by chemical, biological or radiological agents and no risk that an explosive device will detonate prematurely."[302] Carrying out such an attack is also comparatively inexpensive.[303]

In addition, "[c]yberspace is an attractive delivery method for terrorists."[304] "In cyberspace, a single act can inflict damage in multiple locations simultaneously without the attacker ever having physically entered the United States."[305] Consequently, "a

295. *See generally* N.Y. TIMES, July 24, 2005, at Section A (containing articles regarding recent terrorist bombings in London, Egypt, and Iraq).

296. Kornfeld, *supra* note 2, at 482 ("Many dams, aqueducts and pumping stations that capture and carry water over long distances are especially vulnerable to physical damage and would be difficult to replace.").

297. *See* Ware, *supra* note 144, at 127 (many drinking water facilities "have not yet secured their [SCADA] networks and need help in doing so. . .").

298. *Hearing on Creating the Homeland Security Department*, *supra* note 41, at 196 (statement of Samuel G. Varnado) (explaining that "[m]ore vulnerabilities are being found, and consequences of disruptions are increasing rapidly.").

299. *See* Poulsen, *supra* note 138; *cf. see also* Barkham, *supra* note 134, at 62-68 (2001) (describing successful cyber attacks on companies such as AT&T, Yahoo!, Ebay, Amazon.com, as well as the United States Air Force).

300. *See also* Adam Cohen, *When Terror Hides Online*, TIME, Nov. 12, 2001, at 65 ("It's no secret that bin Laden's terrorist army is internet savvy").

301. Brenner & Goodman, *supra* note 135, at 12.

302. *Id.* at 25.

303. *See* Alexander, *supra* note 136, at 86.

304. Brenner & Goodman, *supra* note 135, at 12.

305. NAT'L STRATEGY FOR HOMELAND SECURITY, *supra* note 50, at 34.

terrorist can mount a cyberterror attack from a remote location with little, if any, fear of apprehension."[306] Given the "permeability of cyberspace," tracking down cyber-terrorists is very difficult.[307] Accordingly, cyber-threats to SCADA systems are also likely threats to drinking water security.

iii. CBW

Various biological and chemical contaminants also pose viable threats to drinking water security. A limited number of contaminants

> have the potential to produce widespread death or disease. These contaminants include concentrated pathogens, biotoxins, and a few highly toxic chemicals that remain stable in water long enough to adversely impact public health. A larger group of contaminants could produce localized death or disease in a segment of a population, including several dozen toxic chemicals. Hundreds of contaminants could potentially disrupt service or undermine consumer confidence but would not result in death or disease in the population.[308]

Of the more infamous biological agents, anthrax, plague, and tularemia all remain stable in water.[309] Furthermore, many nonbacterial pathogens are resistant to commonly-used treatment and disinfection methods, such as chlorination.[310] The danger posed by these substances is compounded by the fact that "[t]he common indicators of water quality are of little value in [detecting such contaminants]."[311] Awareness of contamination involving these substances may therefore come long after ". . .affected individuals begin showing signs of adverse health effects."[312]

---

306. Brenner & Goodman, *supra* note 135, at 25.

307. *See id.* at 12.

308. RESPONSE PROTOCOL TOOLBOX, MODULE 1, *supra* note 36, at 12; *see also* EARLY WARNING MONITORING, *supra* note 32, at 9 (explaining that "scientists for the U.S. Army who examined the potential threat of biological warfare agents to potable water concluded that on the basis of existing weaponization, stability in water, and known or potential resistance to chlorine, some of the bacterial agents . . . and all of the biotoxins . . . were potential waterborne threats").

309. *See* EARLY WARNING MONITORING, *supra* note 32, at 22-23 (explaining that anthrax spores are highly resistant to cold, heat, and chemical disinfectants).

310. *See id.* at 9.

311. *Id.* at 22.

312. *Id.* ("[M]anagement of this type of event is related more to medical treatment and response").

Successfully weaponizing biological and chemical agents and using them to contaminate drinking water systems ". . .is far from a trivial undertaking. . ."[313] Other methods of disseminating such weapons, such as by air dispersal, offer much greater chances of successfully causing harm. However, manufacturing and using such weapons against drinking water supplies ". . .it is not so difficult that terrorists. . ." cannot do it.[314] Despite the various technical obstacles preventing terrorists from successfully developing and utilizing NBC weapons, some believe they are capable of overcoming such challenges.[315] CBW are already ". . .within the technical reach of [some] sophisticated terrorist organizations."[316] Accordingly, biological and chemical weapons also threaten drinking water security.

iv. Radiological Contaminants

Lastly, "[c]ontamination of a water supply by radioactivity is possible. . ."[317] Even "[n]atural sources of radioactivity can. . .threaten a supply."[318] However, for various reasons discussed below, "it is increasingly recognized that [other] weapons represent far more credible threats in the hands of terrorists than do nuclear ones."[319] Nevertheless, radiological weapons pose a threat to drinking water infrastructure.

b. Historical Trends

The increasing frequency of terrorist incidents, especially those specifically targeting drinking water infrastructure, further evidences that likely risks to drinking water security exist. As discussed in Section III, terrorists have consistently attempted to attack drinking water supplies using many of the means described above.[320] Incidents involving CBW, such as the October 2001 anthrax attacks, have generally been on the rise since 1995.[321] One of the deadliest terrorist attacks involving CBW oc-

313. Kellman, *supra* note 280, at 729.
314. *Id.*
315. *See* Kellman, *supra* note 75, at 463.
316. *See* TOXIC TERROR, *supra* note 11, at 1.
317. EARLY WARNING MONITORING, *supra* note 32, at 9.
318. *Id.*
319. Sutton, *supra* note 213, at 135; *cf.* Kluger, *supra* note 61, at 39 (discussing the "consensus in Washington" that Al-Qaeda may well have a dirty bomb).
320. *See* 148 CONG. REC. H638-03, *H639 (daily ed. Fed. 28, 2002) (statement of Rep. Tauzin) (discussing the 2002 attempted contamination of the U.S. embassy in Rome and explaining that ". . .it can happen here, too, if we are not careful.").
321. *See* TOXIC TERROR, *supra* note 11, at 2.

curred relatively recently and involved the intentional contamination of drinking water supplies.[322] Although drinking water infrastructure is not always targeted, these incidents nevertheless demonstrate that successful CBW attacks are possible and that terrorists constantly pursue new means to fulfill their goals.[323] "If the trend continues the number of terrorist incidents is likely to keep climbing," and drinking water facilities will increasingly be the target.[324]

The "confluence of two trends" suggests why the threat of CBW terrorism is on the rise: "the growing accessibility of mass-casualty weapons and the emergence of new and more ruthless forms of religious and ideological fanaticism."[325] The "new breed" of terrorist spawned by such fanaticism is not reluctant to use NBC weapons.[326] Such terrorists "pose a real threat of toxic terror," because they have the ". . .motivation to acquire and use chemical or biological weapons. . ." and actively seek out the capability to do so.[327] Unfortunately, this type of terrorist group with "no inhibitions" and "no rules," such as al-Qaeda, is becoming increasingly prevalent.[328] Despite periodic exaggerations by politicians or the media regarding current threats of terrorism, these trends ". . .make it both politically and substantively imprudent. . ." to disregard the threat of terrorism against drinking water infrastructure.[329] Thus, the SDWA Amendments' require-

322. *See* Tucker & Sands, *supra* note 69, at 48 (describing a 1987 incident involving the intentional contamination of a drinking water source with a pesticide that caused the deaths of 19 Philippine army recruits).

323. *See* Fidler, *supra* note 212, at 8 (explaining that "[f]or many Americans, the anthrax attacks were a frightening initiation into a threat that experts. . .have been analyzing since at least the early 1990's"); *see also* Hodge, *supra* note 105, at 256 ("Prior doubts about the potential or ability for an individual or group to intentionally unleash these [biological] agents on an innocent population have been nullified by the brazenness of recent terrorist events").

324. Kornfeld, *supra* note 2, at 447; *see also* Memorandum from R. Nicholas Palarino, *supra* note 99, at 4 ("Intelligence experts believe the threat of biological terrorism has grown sharply in recent years").

325. TOXIC TERROR, *supra* note 11, at 12; *see also* NAT'L STRATEGY FOR HOMELAND SECURITY, *supra* note 50, at 9.

326. *See* TOXIC TERROR, *supra* note 11, at 255 (describing characteristics of terrorist groups willing to use NBC weapons); *cf.* Tucker & Sands, *supra* note 69, at 49 (explaining that historically, "traditional terrorist organizations have eschewed chemical or biological agents").

327. TOXIC TERROR, *supra* note 11, at 9; *see also* Kluger, *supra* note 61, at 39 (describing the "tenacity" of al-Qaeda in seeking radioactive material).

328. *See FBI: Al Qaeda Might Use Poison*, ASSOCIATED PRESS (Sept. 5, 2003), *available at* http://www.cbsnews.com/stories/2003/09/05/national/main571778.shtml.

329. Sokolski, *supra* note 98, at 209; *see also* Julie Bruce, *Bioterrorism Meets Privacy: An Analysis of the Model State Emergency Health Powers Act and the HPAA*

ment that drinking water facilities assess their vulnerabilities against such threats is a prudent course of action.

2. Better Safe Than Sorry

Regardless of what we do understand about how drinking water infrastructure security can be threatened, what we do not understand may be an equally compelling justification for the SDWA Amendments.

a. Nobody Knows What the Likely Threats Are

When it comes to water infrastructure security, "[i]n every conceivable dimension, uncertainty reigns."[330] This uncertainty is itself an overarching vulnerability, as well as cause for concern and caution.[331] Definitive information is lacking regarding such diverse issues as drinking water threat identification and assessment,[332] monitoring and detection capabilities,[333] SCADA systems,[334] hydraulic modeling,[335] and treatment and decontamination technologies.[336] Some insist that the state of our knowledge is so limited, determining whether the risk of a particular

Privacy Rule, 12 ANNALS HEALTH L. 75 (2003) (discussing a CDC report that concluded "terrorist incidents in the United States and elsewhere involving bacterial pathogens, nerve gas, and lethal plant toxins have demonstrated that the United States is vulnerable to biological and chemical threats").

330. Kellman, *supra* note 75, at 488.

331. *See Controlling Bioterror*, *supra* note 19, at 45 (statement of John B. Stephenson).

332. *See* Pat Phibbs, *Decontamination, Water Protection Studies Under Way at EPA Homeland Security Center*, 36 BNA ENV'T REP. 231 (Feb. 4, 2005) (Research is underway ". . .to improve understanding of biologically produced toxins that might be used to contaminate water").

333. *See Utilities Need More Security Information To Guard Against Terrorism, Survey Finds*, 35 BNA ENV'T REP. 331 (Feb. 13, 2004); *see also* Patricia Ware, *Mechanism for Interdisciplinary Research Called Necessary for Security Technology*, 35 BNA ENV'T REP. 284 (Feb. 6, 2004).

334. *See Utilities Need More Security Information To Guard Against Terrorism*, *supra* note 333, at 331.

335. *See generally* WATER SECURITY RESEARCH AND TECHNICAL SUPPORT ACTION PLAN, *supra* note 154, at 21-23.

336. *See Utilities Need More Security Information To Guard Against Terrorism*, *supra* note 333, at 331; *see also* EARLY WARNING MONITORING, *supra* note 32, at 26 ("Research to determine the effectiveness of chlorine and other disinfectants for controlling known biological agents. . .would be very helpful. . ."); *id.* at 9 (". . .the effectiveness of disinfectants on some biowarfare agents is not known"); *id.* at 23.

drinking water threat is significant ". . .would verge on pure speculation. . ."[337]

In addition to the limits of our current comprehension, ". . . threats to water infrastructure are dynamic. . ." and will likely change.[338] ". . .[T]he potential use of chemical and biological agents is an emerging threat and. . .novel agents may be used in the future that have not been considered in past threat assessments."[339] Because of the novel and ever-changing nature of these threats, ". . .it is difficult to extrapolate the probability of such events in the future or to predict their potential impacts."[340] Thus, the SDWA Amendments' cautious and proactive approach to maintaining drinking water infrastructure security is well-founded.

b. Severe Consequences Warrant a Conservative Approach

The potentially devastating consequences of a successful attack on our drinking water infrastructure also dictate that we cannot afford to overlook even unlikely threats.[341] "If there is one lesson to be learned from September 11. . .it is that even the most unlikely events can occur with devastating results."[342] Accordingly, ". . .we should be doing everything we can both to prevent such an action and to prepare for its consequences."[343]

Although it is unlikely that an intentional attack on a drinking water supply could be cause widespread contamination, as discussed above in Section I, the human health consequences of a

337. Kellman, *supra* note 75, at 446; *see also* De Young & Gravley, *supra* note 25, at 147 ("[o]pinions vary on the susceptibility of public water supplies to terrorist attacks as well as the likelihood of such attacks").

338. WATER SECURITY RESEARCH AND TECHNICAL SUPPORT ACTION PLAN, *supra* note 154, at 3; *see also* NAT'L STRATEGY FOR HOMELAND SECURITY, *supra* note 50, at 9 ("Our terrorist enemies are constantly seeking new tactics or unexpected ways to carry out attacks.").

339. WILHEMI & KREMER, *supra* note 98, at 4.

340. *See* TOXIC TERROR, *supra* note 11, at 12; *see also* Kellman, *supra* note 75, at 446 (". . .the direction of biological understanding renders current estimates somewhat irrelevant as to future capabilities.").

341. *See* RESPONSE PROTOCOL TOOLBOX, MODULE 2, *supra* note 62, at 16 (". . .[a]n analysis of potential consequences associated with a particular contamination threat is a complementary effort to the threat evaluation").

342. De Young & Gravley, *supra* note 25, at 147.

343. *Interview With Anthony Lake, Distinguished Professor in the Practice of Diplomacy, Georgetown University*, 6 GEO. PUB. POL'Y REV. 114 (2001) [hereinafter *Lake*].

successful attack ". . .are potentially severe."[344] Furthermore, current environmental and public health monitoring capabilities are likely too slow to evaluate whether a potential threat warrants a response action before significant harm occurs.[345] Therefore, it is appropriate to make conservative assumptions regarding our need for enhanced drinking water infrastructure security measures.[346] The potentially catastrophic consequences of successfully attacking a drinking water system, even if highly unlikely, factor into the need to protect against that possibility.

c. Consumers May Not Care About the Actual Likelihood

Because even "[t]he mere thought that drinking water was tampered with could send a community into a tailspin," a mechanism is needed to assure the public that their drinking water is safe.[347] Public confidence in the safety of their drinking water has little to do with terrorists' actual technical capabilities to contaminate drinking water with CBW. Even the "mere threat of contamination" or simply introducing taste or odor causing substances is enough to cause fear and anxiety.[348] Threats and hoaxes regarding contamination of water supplies "are much more likely" than actual incidents.[349] Consequently, terrorists could fulfill one of their main goals - ". . .instill[ing] fear in the

344. *See* EARLY WARNING MONITORING, *supra* note 32, at 5; *see also* Grace K. Avedissian, *Global Implications of A Potential U.S. Policy Shift Toward Compulsory Licensing of Medical Inventions in A New Era of "Super-Terrorism"*, 18 AM. U. INT'L L. REV. 237, 239 (2002) (discussing the 1995 Tokyo subway Sarin gas attack that left twelve people dead and over five thousand injured).

345. *See* EARLY WARNING MONITORING, *supra* note 32, at 25 (explaining the "loss in sensitivity" in public health reporting during a 1993 cryptospiridium outbreak in Milwaukee, Wisconsin that sickened over 400,000 people).

346. *See* Dagen, *supra* note 212, at 540 ([T]he most efficient as well as most cost-effective way to counter. . ." terrorism is through prevention and preparation).

347. Kornfeld, *supra* note 2, at 471 (explaining that "[i]t is not uncommon for a community to respond hysterically to a real or perceived threat of disease"); *see also* WATER SECURITY WORKING GROUP FINDINGS, *supra* note 30, at i ("[E]ven a credible threat of an attack on water infrastructure could seriously jeopardize the public health and economic vitality of a community").

348. *See* RESPONSE PROTOCOL TOOLBOX, MODULE 2, *supra* note 62, at 10; *see also Hearing on H.R. 3178*, *supra* note 26, at 48 ("Small quantities of toxic chemicals, even if not directly harmful, may cause panic and great economic disruption").

349. *See* EARLY WARNING MONITORING, *supra* note 32, at 8; *see also* RESPONSE PROTOCOL TOOLBOX, MODULE 2, *supra* note 62, at 10 ("[T]he probability of a contamination threat (the mere indication that contamination of the drinking water supply may have occurred) is relatively high").

population. . ." regardless of the actual likelihood of the threat.[350]

Accordingly, the SDWA Amendments provide a beneficial mechanism for reassuring the public that its drinking water is safe. The information gained through completing vulnerability assessments and ERPs can help utility operators expeditiously identify whether a particular threat or hoax is credible, and quickly relate that information to the public, if necessary, to ease concern. Because the SDWA Amendments require the gathering of this vital information, they are a sound legal response.

3. Catastrophic Contamination or Disruption is Unlikely

Although plausible threats to drinking water security exist, the risk of a successful large-scale terrorist attack on America through the water is small.[351] Despite the much-hyped potential "worst-case" consequences, the likeliest threats to drinking water infrastructure actually involve smaller-scale, localized disruptions or contamination incidents.[352] It is "highly unlikely" that such smaller-scale incidents ". . .could ever completely undermine the national security, much less threaten the survival of the United States as a nation."[353]

This conclusion is based upon both the challenges of acquiring and using NBC weapons, as well as their limited ability to cause widespread contamination of drinking water infrastructure.[354] These hurdles deter most would-be terrorists from attempting to use NBC weapons. Similar factors limit the potential for conventional or cyberspace-based attacks to cause catastrophic harm. Moreover, this country's drinking water facilities and regulations

350. RESPONSE PROTOCOL TOOLBOX, MODULE 2, *supra* note 62, at 10; *see also* Kluger, *supra* note 61, at 39.

351. *See* PROTECTING OUR WATER, *supra* note 12, at 11; *see also* RESPONSE PROTOCOL TOOLBOX, MODULE 2, *supra* note 62, at 10 ("Historic evidence suggests that the probability of intentional contamination of the drinking water supply is relatively low. . ."); *see also* EARLY WARNING MONITORING, *supra* note 32, at 22 (The probability of an intentional contamination incident is "extremely low. . .").

352. *See* Gertz, *supra* note 123, at A1 (most attacks by al-Qaeda ". . .will be small-scale, incorporating relatively crude delivery means and easily produced or obtained chemicals, toxins or radiological substances. . ."); *see also* TOXIC TERROR, *supra* note 11, at 253 (". . .[T]he most probable terrorist use of CBW agents will be tactical and relatively small-scale").

353. *See, e.g.*, Sokolski, *supra* note 98, at 218.

354. *See* Brenner & Goodman, *supra* note 135, at 8 (it is simply ". . .far more difficult to obtain and deploy chemical, biological, radiological, and nuclear agents than conventional explosives"); *see also id.* (". . .it is generally more difficult to calculate and direct the effects of chemical and biological agents. . .").

are already structured to prevent pathogenic and radiological drinking water contaminants from reaching consumers.[355] Thus, just because contaminants such as chemical and biological agents ". . .are often described as 'weapons of mass destruction' does not mean that the ability to inflict mass casualties is an inherent property."[356]

a. Technical Challenges of NBC Weapons

i. Radiological and Nuclear Weapons

It is "very difficult" for terrorists to acquire and refine the fissile material necessary to develop a nuclear or radiological weapon.[357] In addition, although there are noted exceptions, few terrorists or people willing to assist terrorists have the ". . .very high degree of technical capability" needed to manufacture a workable nuclear or radiological weapon.[358] Because of these challenges, radiological and nuclear weapons have never before been used to attack drinking water supplies and remain only ". . .mere possibilities in the arsenal of 'physical world' delivery methods."[359]

ii. Chemical Weapons

Chemical agents are ineffective at producing the mass-casualties or widespread destruction that fanatical terrorists often seek to accomplish.[360] Terrorists seeking to use chemical weapons ". . .have to overcome significant technical hurdles and. . .run major safety risks. . ."[361] Producing chemical weapons ". . .is not as easy as is often suggested in media accounts."[362] The synthesis

355. *See, e.g.*, 40 C.F.R. § 141.63 (listing maximum contaminant levels for microbiological contaminants); 40 C.F.R. § 141.66 (listing maximum contaminant levels for radionuclides); 40 C.F.R. § 141.72 (listing disinfection requirements for public water supplies).

356. TOXIC TERROR, *supra* note 11, at 254; *see also* Tucker & Sands, *supra* note 69, at 52 (explaining that "[i]n very few cases did the perpetrators seek to inflict mass-casualties – defined as 1,000 or more deaths – and in none did they occur.").

357. *See* NAT'L STRATEGY FOR HOMELAND SECURITY, *supra* note 50, at 9 ("[A]cquiring or refining a sufficient quantity of fissile material is very difficult – though not impossible.").

358. *See id.*

359. Brenner & Goodman, *supra* note 135, at 8.

360. *See* TOXIC TERROR, *supra* note 11, at 6 (discussing how an explosive device would have caused more casualties than the poor quality sarin gas used in the 1995 Aum Shinriko Tokyo attacks).

361. *Id.*

362. *Id.*

of nerve agents such as sarin and VX requires the use of highly reactive and corrosive ingredients that may be difficult to acquire and are dangerous to handle."[363] Because ". . .the production of chemical agents runs the risk of killing the producers," it is a natural deterrent to their use.[364]

The challenges of acquiring and producing chemical agents are compounded by the fact that ". . .it takes massive amounts of chemical agent to produce military casualties with any reliability, and maximizing their. . .dissemination is no easy task."[365] This is especially true for drinking water given the effect of dilution in large drinking water reservoirs. Although standard industrial tanks can be used for storage, producing and maintaining sufficient quantities of chemical agents increases the likelihood that the terrorist enterprise will be discovered and stopped.

Moreover, exposure to water or chemical neutralization processes renders certain chemical weapons, such as nerve agents, ineffectual.[366] Volatile chemical agents, such as sarin, are also vulnerable to evaporation from sun and heat.[367] Chlorination appears to destroy other chemical weapons, such as mustard agents.[368] These factors explain why chemical agents ". . .injure far more than they kill" and why they "have been used so rarely even in war."[369] Accordingly, while it is possible to contaminate a portion of a drinking water supply with chemical agents, it is very difficult and the consequences would likely be limited.[370]

---

363. *Id.*

364. Sokolski, *supra* note 98, at 213.

365. *Id.* at 211 (explaining that the amount of chemical or nerve agents needed to produce mass-casualties "would still be measured in tons"); *see also id.* at 212 ("Technically, dissemination of chemicals to produce massive casualties is difficult. . .").

366. *See* WILHEMI & KREMER, *supra* note 98, at 5.

367. *See* Sokolski, *supra* note 98, at 211.

368. *See* WILHEMI & KREMER, *supra* note 98, at 4 ("Mustard agents can. . .be readily oxidized using chlorine bleach"); *see also id.* at 12 (discussing effectiveness of bleach-based products for both chemical and biological agents).

369. Sokolski, *supra* note 98, at 211-12 (explaining that "if military use of chemical and biological agents has been historically rare, domestic criminal and terrorist use of them has been rarer still").

370. *See Hearing on Terrorism: Are America's Water Resources and Environment at* Risk, *supra* note 36, at 51 (statement of Ronald L. Dick) ("Affecting a city-sized population by a hazardous industrial chemical attack on a drinking water supply is not credible").

iii. Biological Weapons

"The technical challenges of terrorists using traditional biological agents to produce massive fatalities [via drinking water] are no less daunting."[371] It is actually ". . .much harder to develop a biological weapon than a chemical weapon, and much, much harder than using computers for terrorist action."[372] As with the raw materials for producing chemical weapons, obtaining the necessary strains of pathological agents to manufacture a biological weapon is not easy.[373] Terrorists cultivating such infectious agents always run the risk of infecting themselves, a suicidal drawback.[374] In addition, "[t]he difficulty in producing enough of the agent to create a weapon may present an important limitation to terrorism. . .."[375]

As with chemical agents, the effects of dilution, exposure to various environmental factors, and the routine treatment processes that drinking water undergoes will also likely destroy the pathological effect of most biological agents.[376] Moreover, even if a drinking water supply is successfully contaminated with a biological agent, most biological agents ". . .are neither uniformly fatal nor directly communicable: if most victims got effective medical care. . .most would survive."[377] Of course, it is cold comfort to consumers that their contaminated drinking water will only injure and not kill them.

Attacks involving aerosolized biological weapons represent more of a threat to public health than ingestion of contaminated

---

371. Sokolski, *supra* note 98, at 213 (explaining that the FBI has "yet to find a terrorist organization that has built an effective mass-casualty biological agent delivery system").

372. *Lake*, *supra* note 343, at 114 ("[I]f you're calculating probabilities, then bioterrorism. . .is relatively unlikely."); *see also* Copeland & Cody, *supra* note 3, at 3 (discussing the relevant characteristics regarding an agent's "potential as a biological weapon include[ing] its stability in a drinking water system, virulence, culturability in the quantity required, and resistance to detection and treatment").

373. *See* TOXIC TERROR, *supra* note 11, at 7; *see also* WILHEMI & KREMER, *supra* note 98, at 5 (explaining that viruses are very difficult to weaponize).

374. *See* TOXIC TERROR, *supra* note 11, at 7.

375. Kellman, *supra* note 75, at 440 (". . .[L]arge volumes of highly concentrated material are required for a biological weapon.").

376. *See* Sokolski, *supra* note 98, at 213 ("Sunlight kills or denatures most biological agents . . . ."); *see also* EARLY WARNING MONITORING, *supra* note 32, at 9 ("Most bacterial pathogens have been reported to be destroyed by common disinfectants such as . . . chlorine.").

377. Richards, *supra* note 28, at 11308; *see also Progress in Treating Deadly Ebola*, THE AGE (Dec. 12, 2003), *at* http://www.theage.com.au/articles/2003/12/12/1071125633389.html?from=storyrhs (reporting on progress in treatments for Ebola virus).

drinking water.[378] However, showering in water contaminated with CBW may have precisely this effect.[379] Thus, the technical challenges associated with using biological weapons to contaminate drinking water supplies are not a license for drinking water facilities to ignore this threat.

Nevertheless, CBW attacks on water systems are most likely not capable of inflicting ". . .the mass-death predicted by the most alarmist scenarios."[380] Despite the "waves of concern" generated by the media, the potential for terrorists to contaminate drinking water supplies with CBW agents is "not something for ordinary Americans to get excited about."[381] ". . .[T]he difficulties of acquiring and deploying chemical and biological agents and their poor past performance as compared to high explosives would weigh heavily against their initial selection" by a terrorist group.[382] The basic technology for developing chemical and biological weapons "has been available in the open literature for more than half a century."[383] So, if such attacks have not happened yet, ". . .there must be reasons."[384] These reasons suggest that ". . .our water supply is safe. . ." from large-scale attacks involving NBC weapons.[385]

---

378. *See* EARLY WARNING MONITORING, *supra* note 32, at 8-9; *see also* TOXIC TERROR, *supra* note 11, at 8 (explaining that aerosolization is the "[t]he only potential way to inflict mass casualties with a [biological weapon] . . . ."); *see also* Sokolski, *supra* note 98, at 213.

379. *See* U.S. ENVTL. PROT. AGENCY, RESPONSE PROTOCOL TOOLBOX: PLANNING FOR AND RESPONDING TO DRINKING WATER CONTAMINATION THREATS AND INCIDENTS, INTERIM-FINAL, MODULE 5: PUBLIC HEALTH RESPONSE GUIDE at 29 (Apr. 2004) ("[C]hemical and biological agents likely to become suspended in air are more likely to pose a risk to public health through inhalation pathways (e.g., while showering).").

380. TOXIC TERROR, *supra* note 11, at 253.

381. *Interview With Matthew Meselson, supra* note 227, at 107 (explaining that the number of people who have died from bioterror incidents is negligible compared to the number killed each year by accidental shootings or natural disasters); *see also* Tucker & Sands, *supra* note 69, at 48 (describing a "tendency of U.S. government officials to exaggerate the threat of chemical and biological terrorism [that] has been reinforced by sensational reporting in the press and an obsessive fascination with catastrophic terrorism in Hollywood films").

382. Sokolski, *supra* note 98, at 214; *see also* Carol Morello and Spencer S. Hsu, *Senate Offices to Begin Reopening: Police Say No Link Found in Dirksen Ricin, Earlier Letter to White House*, WASHINGTON POST, Feb. 5, 2004, at A01 (discussing failed ricin attacks on the Dirksen Senate and White House).

383. *Interview With Matthew Meselson, supra* note 227, at 108.

384. *Id.*; *see also* TOXIC TERROR, *supra* note 11, at 9 (discussing the Aum Shinrikyo cult's 10 failed attempts to conduct terror attacks using anthrax and botulinum toxin).

385. *See* 147 CONG. REC. S13902-03 (daily ed. Dec. 20, 2001) (statement of Sen. Smith).

iv. Conventional Weapons

Conventional explosives represent the most significant concern to drinking water facility managers.[386] Nevertheless, there are still inherent limits to terrorists' ability to threaten drinking water infrastructure with these weapons. To cause maximum effect, a conventional attack would have to target a centralized facility, such as a major treatment plant or pumping station.[387] Since the effectiveness of explosives ". . .depends on their proximity to the physical target, conventional explosives have to be deployed in an area that is relatively near the target, an endeavor that can attract unwanted attention or otherwise raise the risk of apprehension, failure or death."[388] Security can be focused around these key points or "critical nodes" to maximize the chances that an attempted terrorist attack will be thwarted.[389]

The destruction of satellite drinking water infrastructure components, such as major intake pipes or pumping stations, could seriously affect drinking water availability. However, as drinking water infrastructure elements reach into increasingly more localized service areas, such as neighborhood water mains, the consequences of damage to or destruction of these components also become more limited and easily repaired.[390] These smaller infrastructure components and facilities are therefore less attractive targets.[391] Consequently, while conventional weapons pose the likeliest threat to drinking water infrastructure, there are factors that hinder terrorists' ability to successfully execute such attacks.

b. Drinking Water Infrastructure Vulnerability is Limited

In addition to the intrinsic limitations of various weapons' ability to threaten drinking water security, only certain drinking water infrastructure components are realistically vulnerable to attack.[392] These components include post-treatment storage res-

386. *See* TOXIC TERROR, *supra* note 11, at 253.

387. *See* EARLY WARNING MONITORING, *supra* note 32, at 9.

388. Brenner & Goodman, *supra* note 135, at 11.

389. *See Hearing on Terrorism: Are America's Water Resources and Environment at* Risk, *supra* note 36, at 51 (statement of Ronald L. Dick).

390. *See* EARLY WARNING MONITORING, *supra* note 32, at 9 ("Although the destruction of major pipes will disrupt service, pipes can usually be repaired within days.").

391. *See* Copeland & Cody, *supra* note 3, at 2 ("[T]he large number of small systems. . .are less likely to be perceived as key targets . . . .").

392. *See Hearing on Terrorism: Are America's Water Resources and Environment at* Risk, *supra* note 36, at 51 (statement of Ronald L. Dick) ("In reality, targeting the

ervoirs, distribution reservoirs, and water mains.[393] Moreover, drinking water facilities are already designed to protect public health by preventing contaminated drinking water from reaching consumers. These factors further diminish the ability of terrorists to successfully cause catastrophic contamination or disruption to drinking water systems.

i. Distribution Networks

Distribution networks are perhaps the most vulnerable drinking water infrastructure system component.[394] These systems could potentially be exploited to ". . .spread highly concentrated amounts of poison to a few thousand homes or businesses."[395] This is in part due to their extreme complexity and magnitude.[396] Distribution systems can be comprised of networks of thousands of miles of pipes, pumps, and storage tanks that carry drinking water 'downstream' from reservoirs and treatment centers and deliver it on demand to homes, commercial establishments, and industries.[397] Once distributed to a home or business, contaminated water from the distribution network could potentially reach and affect point-of-use/point-of-entry devices, such as washing machines, dishwashers or water heaters.[398]

---

water supply may prove difficult."). *See* EARLY WARNING MONITORING, *supra* note 32, at 8.

393. *See* EARLY WARNING MONITORING, *supra* note 32, at 8.

394. *See* EXPERTS' VIEWS ON HOW FEDERAL FUNDING CAN BEST BE SPENT TO IMPROVE SECUIRTY, at 8, *reprinted in Controlling* Bioterror, *supra* note 137, at 49 (citing a government survey finding that nearly 75% of drinking water experts believe the distribution system of a drinking water facility is a significant vulnerability); *see also* Kornfeld, *supra* note 2, at 447-48 ("Generally, there are two areas of vulnerability identified by experts: the pre-treatment and water intake part of the system; and 'the distribution system post-treatment . . . .").

395. Harris, *supra* note 15, at 1.

396. *See* RESPONSE PROTOCOL TOOLBOX, MODULE 1, *supra* note 36, at 22 ("Distribution systems are particularly unique in that many are a complex, and often undocumented, mix of relatively new and old components").

397. *See Hearing on H.R. 3178*, *supra* note 26, at 47 (statement of Richard G. Luthy); *see also* EXPERTS' VIEWS ON HOW FEDERAL FUNDING CAN BEST BE SPENT TO IMPROVE SECURITY at 8, *reprinted in Controlling* Bioterror, *supra* note 137, at 49 (discussing one metropolitan distribution network comprised of nearly 7,100 miles of water mains).

398. *See* WATER SECURITY RESEARCH AND TECHNICAL SUPPORT ACTION PLAN, *supra* note 154, at 22 (explaining that contaminants could potentially be trapped inside these devices causing lingering health risks after the main distribution system components are decontaminated).

Because of their multiple access points, preventing the introduction of contaminants into distribution networks is difficult.[399] Furthermore, because water in the distribution system has already been treated and is on its way to the consumer, the protective effects of dilution and treatment are diminished.[400] The proximity of water in the distribution network to consumers would render contamination ". . .virtually undetectable until it was too late to prevent harm."[401] Consequently, "[o]ne wacko who understands hydraulics and (has) access to a drum of toxic chemicals could inflict serious damage to a water supply in a neighborhood or pressure zone without detection pretty quickly in most communities."[402]

The vulnerability of distribution networks is cause for concern and appropriate legislative responses, such as the SDWA Amendments. However, it is not cause for panic. Despite the ongoing need for "real-time" monitoring, water in the distribution system is routinely monitored to ensure its safety.[403] In addition, maintaining a chlorine residual in the distribution network, and increasing it in times of perceived threats, may still be sufficient to inactivate many chemical and biological agents.[404]

Furthermore, contamination or disruption of local distribution system components will, by nature, affect increasingly confined areas. These localized impacts are easier to isolate and ad-

399. *See* EXPERTS' VIEWS ON HOW FEDERAL FUNDING CAN BEST BE SPENT TO IMPROVE SECURITY, at 8, *reprinted in Controlling* Bioterror, *supra* note 137, at 49; *see also Controlling Bioterror, supra* note 137, at 57 (explaining that contaminants can easily be put into the system via fire hydrants); *see also* WATER SECURITY RESEARCH AND TECHNICAL SUPPORT ACTION PLAN, *supra* note 154, at 9 ("Among the key vulnerabilities are. . .the ease of introducing contaminants to wellheads and distribution systems. . .").

400. *See* EXPERTS' VIEWS ON HOW FEDERAL FUNDING CAN BEST BE SPENT TO IMPROVE SECURITY, at 8, *reprinted in Controlling* Bioterror, *supra* note 137, at 49; *see also* EARLY WARNING MONITORING, *supra* note 32, at 9 (explaining that doses of contaminants in distribution networks may be targeted close enough to consumers to cause health effects).

401. *Id.* ("[L]imited technologies are readily available that can detect a wide range of contaminants once treated water is released."); *see also* PROTECTING OUR WATER, *supra* note 12, at 8 (The first indications of such an attack "could be an increase in taste or odor complaints by customers," or in the worst-case, "an increase in emergency room visits.").

402. De Young & Gravley, *supra* note 25, at 146 (quoting Gay Porter DeNileon, National Critical Infrastructure Protection Advisory Group member).

403. *See* EARLY WARNING MONITORING, *supra* note 32, at 23 ("Distribution systems are routinely monitored to determine whether the integrity of the system is being maintained and the quality of the water is in compliance with water quality standards").

404. *See* id. at 9.

dress.[405] Distribution systems may also have structural features that enable further isolation of the contaminated area.[406] Thus, as long as drinking water networks are designed to have redundant distribution routes, the disruption and harm caused by such an attack can be minimized.[407] This is, again, cold comfort to those in affected buildings or neighborhoods. However, it once again illustrates that certain factors limit terrorists' ability to completely incapacitate our drinking water infrastructure, even by attacking its most vulnerable components.

ii. Sourcewater and Supply

It is unlikely that a sufficient quantity of contaminant could be intentionally introduced into a source waterbody so as to cause great harm. The effects of dilution and normal treatment processes for ". . .chemical, biological, or radiological contaminants in source waters will, in many cases, reduce the concentration to below levels of concern. . ." for all but "truck-load quantities" of contaminants.[408] Source waterbodies often involve such large volumes of water that it can take days or even weeks to reach consumers.[409] Normal treatment processes, ". . .such as chlorination and filtration are designed to kill pathogens. . .and probably would be equally effective against a deliberately released agent."[410] Consequently, targeting a source waterbody ". . .is not a very effective way to contaminate drinking water."[411]

While the risk of successfully threatening public health by intentionally contaminating a source waterbody is extremely low,

---

405. *See id.*

406. *See* RESPONSE PROTOCOL TOOLBOX, MODULE 1, *supra* note 36, at 22; *cf.* EARLY WARNING MONITORING, *supra* note 32, at 28 (discussing problems many drinking water plants have in taking actions, such as shutting down intakes, while attempting to isolate potentially contaminated water).

407. *See* EARLY WARNING MONITORING, *supra* note 32, at 9.

408. WATER SECURITY RESEARCH AND TECHNICAL SUPPORT ACTION PLAN, *supra* note 154, at 23; *see also Hearing on H.R. 3178*, *supra* note 26, at 48 (statement of Richard G. Luthy); *see also* De Young & Gravley, *supra* note 25, at 146-47 (discussing the "dilution effect"); Kellman, *supra* note 75, at 443 ("Contamination of water supplies is considerably more difficult. . .because of the extraordinary quantities of pathogens necessary and because filtration and chlorinated purification systems would likely kill the agent."); EARLY WARNING MONITORING, *supra* note 32, at 9 (The threat of successfully contaminating water supplies is ". . .much less likely owing to the effects of dilution and treatment").

409. *See* EXPERTS' VIEWS ON HOW FEDERAL FUNDING CAN BEST BE SPENT TO IMPROVE SECURITY at 8, *reprinted in Controlling* Bioterror, *supra* note 137, at 49.

410. TOXIC TERROR, *supra* note 11, at 7.

411. *See Controlling Bioterror*, *supra* note 19, at 57.

drinking water sources and reservoirs remain tantalizing terrorist targets. Consequently, "government cannot afford to be complacent about the potential for high-casualty chemical and biological attacks."[412] Watersheds and drinking water reservoirs cover vast areas making it "difficult to maintain security."[413] Pilots have been quoted as saying that ". . .it's easy to glide over a reservoir and dump hundreds of pounds of hazardous chemicals. . ." into it.[414]

In addition, ". . .some infectious agents and a few biotoxins are unaffected by chlorination."[415] Relatively recent outbreaks of waterborne illness demonstrate that our treatment systems are not flawless.[416] Furthermore, unlike more common biological pathogens that ". . .can be easily detected within minutes. . ." at high doses, such as cholera or typhoid, current monitoring and detection capabilities for CBW are much less certain.[417] Intentional contamination incidents will also most likely have no telltale precursor events, such as large rainfalls or natural disasters, that facility operators sometimes use to predict the increased presence of common pathogens in water supplies. Thus, despite the challenges associated with successfully contaminating a source waterbody, ". . .complacency over the microbiological safety of U.S. drinking water may be imprudent."[418]

---

412. Tucker & Sands, *supra* note 69, at 52.

413. *See* EXPERTS' VIEWS ON HOW FEDERAL FUNDING CAN BEST BE SPENT ON IMPROVING SECURITY at 8, *reprinted in Controlling* Bioterror, *supra* note 137, at 49; *see also* Kornfeld, *supra* note 2, at 454-55 (discussing Tampa, Florida's difficulties in patrolling their source water reservoir); *cf.* De Young & Gravley, *supra* note 25, at 147 ("[I]t may be relatively easy to protect water sources and treatment plants from contamination . . . .").

414. *See* Kornfeld, *supra* note 2, at 452 (citing *Flights over NYC reservoirs causing concern*, WATERTECH ONLINE (July 3, 2002), *at* http://www.watertechonline.com/news.asp?mode=4&N_ID=32600 (quoting an amateur pilot as saying "I could have just opened the window and dumped anything into the water")); *cf. id.* at 456 (discussing state laws and federal aviation association guidance disapproving of reservoir "fly-overs").

415. De Young & Gravley, *supra* note 25, at 147; *cf. Hearing on H.R. 3178*, *supra* note 26, at 49 (discussing advances in membrane, sorptive, and oxidative treatment technologies).

416. *See* Kornfeld, *supra* note 2, at 468 (discussing the 1993 Milwaukee cryptosporidiosis outbreak that sickened over 400,000 people and contributed to over 100 deaths despite disinfection and filtration of the water).

417. *See* EARLY WARNING MONITORING, *supra* note 32, at 9; *see also id.* at 26 ("[T]here is a need for the development of new methods to rapidly detect and identify a broad spectrum of pathogens and biotoxins."); Kellman, *supra* note 75, at 428 ("Pathogens are undetectable or nearly so.").

418. *See* Kornfeld, *supra* note 2, at 468.

iii. Current System Protections

The fundamental mission of drinking water system operators is to protect public health by preventing contaminated water from reaching consumers. This is also the basic goal of existing drinking water regulatory standards that have been put in place for dozens of organic, inorganic, pathogens, and radiological contaminants.[419] These efforts have ensured that U.S. drinking water is among the safest in the world. "[T]he types and extent of contamination and the health effects resulting from physical acts of terrorism are often – but not always – similar to the consequences of traditional system contamination that concern water system managers every day."[420] Thus, while some aspects of the threats currently facing drinking water systems are new, drinking water facilities are already designed to ". . .[accommodate] the kinds of analysis, planning, and response necessary to counter a deliberate attack."[421]

"Traditionally, water systems have protected public health and ensured safe water by implementing a 'multiple barrier' approach to preventing contamination."[422] "In this approach systems place as many 'barriers' as reasonably possible between the risks. . .and the consumer."[423] Thus, public health protection is ". . .not dependent on one process but several in a train that provide backup protection."[424] Barriers are physical, such as source water protection measures, fencing and restricted access to other

419. *See, e.g.*, 42 U.S.C. § 300g-1(b)(4)(A) (2006) (requiring "maximum contaminant level goals" to be set "at the level at which no known or anticipated adverse effects on the health of persons occur . . . ."); *see also generally* 40 C.F.R. §§ 141(B), 141(G) (establishing maximum contaminant levels for drinking water).

420. *See Oversight Hearings On Drinking Water System Security*, *supra* note 178; *see also* EARLY WARNING MONITORING, *supra* note 32, at 23 ("It would appear from the limited data available that the organisms known to be warfare agents would probably be controlled under emergency conditions using the same crisis management practices currently used to respond to waterborne disease outbreaks caused by other microbes.").

421. *See Oversight Hearings On Drinking Water System Security*, *supra* note 178; *see also* EARLY WARNING MONITORING, *supra* note 32, at 26 ("Management practices for controlling natural and deliberate contaminating events appear to be sufficient for responding to microbial hazards in drinking water and minimizing the health effects . . . .").

422. *See Oversight Hearings On Drinking Water System Security*, *supra* note 178; *see also Hearing on H.R. 3178*, *supra* note 26, at 49 (statement of Richard G. Luthy) ("[A] fundamental design paradigm is to install multiple barriers . . . .").

423. *See Oversight Hearings On Drinking Water System Security*, *supra* note 178 ("[T]his approach parallels the classic physical security triad: 'Detect, delay, respond.").

424. *Hearing on H.R. 3178*, *supra* note 26, at 49 (statement of Richard G. Luthy).

key infrastructure components, as well as adequate treatment processes.[425] Barriers also include institutional measures, such as proper ". . .operation, maintenance, and management by committed and well-trained staff."[426] The "key" to providing safe drinking water and protecting public health lies in the ability of drinking water systems to maintain this multiple barrier system.[427]

However, the effectiveness of the multiple barrier paradigm is limited by "single points of failure" and the potential for "end-runs."[428] First, "[m]any drinking water systems are 'linear' – that is, they have single transmission lines leading into the treatment facility and single pumping stations along the system, and often use a single computer operating system."[429] Thus, although each of the components together might comprise of system of multiple barriers, problems at any of these "single points of failure" could render a system inoperable.[430] Second, there are practical limits to how far along the supply and distribution chain multiple barriers can be put in place. At some point, such as in the distribution network, water will be beyond one or more of the multiple layers of protection.[431] Introducing contaminants at a point past these barriers, therefore, nullifies their protective potential. Accordingly, as confirmed by recent outbreaks of waterborne illness, the multiple barrier system is not impenetrable.[432]

---

425. *See Oversight Hearings On Drinking Water System Security*, *supra* note 178; *see also* ASSET BASED VULNERABILITY CHECKLIST, *supra* note 118, at 3 ("The first line of defense is to deny or delay access.").

426. *See Oversight Hearings On Drinking Water System Security*, *supra* note 178.

427. *See id.*

428. *See* EARLY WARNING MONITORING, *supra* note 32, at 9 ("[t]he main lines of defense against physical and cyber acts of destruction and contamination include the design of a redundant water treatment and distribution system and denial of access").

429. EXPERTS' VIEWS ON HOW FEDERAL FUNDING CAN BEST BE SPENT TO IMPROVE SECURITY, at 9, *reprinted in Controlling* Bioterror, *supra* note 137, at 49.

430. *See id.* at 7-9, *reprinted in Controlling* Bioterror, *supra* note 137, at 49 (discussing the various potential single points of failure for drinking water facilities); *see also* WATER SECURITY RESEARCH AND TECHNICAL SUPPORT ACTION PLAN, *supra* note 154, at 13 (explaining the potential "cascading effect" that could be caused by the extensive interconnectedness of water system components).

431. *See Hearing on H.R. 3178*, *supra* note 26, at 49 ("[W]e need to extend the multiple barrier concept to. . .extend from the water treatment plant to include the distribution system and point of use.").

432. *See* Kornfeld, *supra* note 2, at 468 (discussing the 1993 Milwaukee cryptosporidiosis outbreak).

4. We Can Contaminate Our Own Drinking Water, Thank You

From a relative risk standpoint, debating the likelihood and consequences of terrorist threats to drinking water infrastructure may seem like a misguided exercise. The risk terrorism poses to drinking water safety almost indisputably pales in comparison to the threats drinking water supplies face everyday from pollution, overuse, and lack of adequate funding for infrastructure maintenance. The unfortunate truth is that plenty of bad stuff gets into our drinking water already.

Thousands of illnesses and hundreds of deaths occur each year, not as the result of terrorist efforts, but because of commonly-found waterborne contaminants.[433] Microbial hazards are present in our drinking water due to noncompliance with drinking water regulations, natural events, such as floods and toxic algal blooms, and unintentional catastrophic events, such as untreated sewage overflows.[434] Various non-biological waterborne contaminants also are present in our drinking water such as lead,[435] arsenic,[436] perchlorate,[437] as well as the gasoline additive, methyl

---

433. *See* EARLY WARNING MONITORING, *supra* note 32, at 26 (citing Center for Disease Control estimates of up to 900,000 illnesses and possibly 900 deaths caused each year in the U.S. "as a result of waterborne microbial infections"); *see also* Kornfeld, *supra* note 2, at 467 ("Over the past decade a number of outbreaks, in the U.S., involving . . . Cryptosporidiosis (Crypto), have sickened at least 500,000 and killed hundreds."); *see also* Steve E. Hrudey & Richard Walker, *Walkerton – 5 Years Later: Tragedy Could Have Been Prevented*, OPFLOW (Am. Water Works Assoc., Denver, Co.), June 2005, at 1 (discussing serious flaws within an Ontario municipal drinking water system that "aligned to permit a breakthrough of *E. coli*. . .causing seven deaths and more than 2,300 cases of waterborne disease").

434. *See* EARLY WARNING MONITORING, *supra* note 32, at 22; *see also* Patricia Ware, *EPA Says Utilities Met Federal Standards for 90 Percent of Consumers in Fiscal 2004*, 36 BNA ENV'T REP. 1040 (May 20, 2005) (discussing an EPA Inspector General memorandum "saying the agency has consistently . . . overstated the quality of drinking water in the United States . . . .").

435. *See* David Nakamura, *Water in D.C. Exceeds EPA Lead Limit*, WASHINGTON POST, Jan. 31, 2004, at A01 (discussing "serious" health effects caused by lead exposure and explaining that two-thirds of homes tested had water that exceeded federal drinking water limits for lead).

436. *See* Patricia Ware, *Many Private Wells in New Hampshire Exceed Federal Standard for Arsenic*, 34 BNA ENV'T REP. 2250 (Oct. 10, 2003); *see also* Michael C. White, *The EPA's new arsenic standard for drinking water*, TRENDS (Am. Bar Assoc. Section of Env't, Energy, and Natural Res., Chicago, IL.), March/April 2002, at 8-9 (discussing prevalence and health effects of arsenic); Patricia Ware, *Drinking Water: EPA's Multi-Year Research Strategy To Focus on Arsenic, Disinfection Byproducts*, 34 BNA ENV'T REP. 2704 (Dec. 12, 2003) ("Small systems that must treat for arsenic are expected to have problems affording the technology.").

tertiary butyl ether ("MTBE").[438] Amazingly, even "[c]hemicals intentionally introduced for water disinfection historically have posed more of a health threat than acts of chemical or biological sabotage."[439]

These problems may not be surprising given that the condition of our existing drinking water infrastructure is ". . .barely passing. . ."[440] Aside from complex distribution networks or open reservoirs, our antiquated drinking water infrastructure is a key vulnerability.[441] ". . .[M]any components of our water systems are aging and need repairs, replacements, or upgrades. . ."[442] Accordingly, the issues facing our drinking water infrastructure on a daily basis pose ". . .a bigger threat to the American population" than terrorist attacks.[443]

Addressing all of these issues could cost billions, and there is stiff competition for limited funding.[444] Thus, there is a danger that unwarranted homeland security spending will reduce the resources available for addressing truly pressing public health concerns.[445] In some instances, ". . .the investment in homeland security will result in public safety benefits; water testing to de-

437. *See* Patricia Ware, *Drinking Water: EPA Sets Reference Dose for Perchlorate Based on National Academies Suggestion*, 36 BNA ENV'T REP. 377 (Feb. 2, 2005).

438. *See* Patricia Ware, *Drinking Water: Study Estimates Cost of MTBE Remediation At Up to $3 Billion; Utilities Dispute Figures*, 36 BNA ENV'T REP. 1242 (June 17, 2005).

439. De Young & Gravley, *supra* note 25, at 147; *see also* EARLY WARNING MONITORING, *supra* note 32, at 9 ("The use of chlorine must also be balanced with concerns about the formation of chlorinated by-products").

440. *See Infrastructure: Drinking Water, Wastewater Facilities Get Poor Grades by Engineering Group in Report*, 36 BNA ENV'T REP. 489 (Mar. 11, 2005) (discussing a "report card" released by the American Society of Civil Engineers giving the condition of the nation's drinking water infrastructure a grade of D-).

441. *See* WATER SECURITY RESEARCH AND TECHNICAL SUPPORT ACTION PLAN, *supra* note 154, at 9; *see also* Meredith Preseton, *Bill to Improve Communication About Lead Will Be Introduced Soon, Jeffords Tells Panel*, 35 BNA ENV'T REP. 769 (Apr. 9, 2004) (quoting comments of Sen. Michael Crappo that "most public water systems. . .are 40 -140 years old").

442. *Hearing on H.R. 3178*, *supra* note 26, at 47.

443. *See* Dagen, *supra* note 212, at 537; *see also* EARLY WARNING MONITORING, *supra* note 32, at 22 (These common sources of contamination "have a high potential to cause large outbreaks of disease in exposed populations.").

444. *See* Susan Bruninga, *Cost of Necessary Clean Water Projects Estimated at $181 Billion, EPA Survey Says*, 34 BNA ENV'T REP. 1949 (Sept. 5, 2003); *see also* Ware, *supra* note 436, at 1242.

445. *See* NAT'L STRATEGY FOR HOMELAND SECURITY, *supra* note 50, at 64; *see also* Raimo Väyrynen, *Environment, Violence, and Political Change*, 15 Notre Dame J. L. Ethics & Pub. Pol'y 593, 613 (2001) ("[L]ooming security threats are easily exaggerated and various defensive remedies to potential terrorist actions could be an expensive and misguided cure.").

tect chemical or biological agents, for example, will improve overall water quality."[446] However, investing in solutions to these more common drinking water threats could also significantly improve drinking water security.[447] Consequently, appropriations decisions must consider whether the cost-benefits of addressing existing threats to drinking water safety outweigh those posed by terrorism.[448]

A successful catastrophic attack on our nation's critical drinking water infrastructure is unlikely and other common threats pose much greater risks of harm. However, we cannot afford to be complacent about drinking infrastructure security. Certain weapons can threaten drinking water safety, certain infrastructure components are vulnerable to these threats, and the consequences of even a successful small-scale attack could be devastating.

Furthermore, terrorism poses an ever-changing threat. Consequently, our past experience will not necessarily help us predict future attacks.[449] Terrorists are morbidly creative and ". . .highly prone to imitation, so that an innovation. . .typically spawns a string of 'copycat' incidents."[450] One enterprising terrorist could overcome the technical obstacles of contaminating or disrupting drinking water supplies and "open the door" for others.[451] As a result, the SDWA Amendments' requirements are warranted to ensure that drinking water infrastructure security is not jeopardized by the threats of terrorism.

---

446. NAT'L STRATEGY FOR HOMELAND SECURITY, *supra* note 50, at 64; *see also* Ware, *supra* note 331, at 284 ("[S]ecurity technology could help detect accidental contamination, help in routine monitoring, help protect aquatic species, and increase consumer confidence.").

447. *See Five Opportunities to Improve Security Identified by Environmental Law Institute*, 34 BNA ENV'T REP. 2762 (Dec. 19, 2003) (discussing "five areas in which conventional activities can be linked to homeland security efforts to improve drinking water . . . .").

448. *See* NAT'L STRATEGY FOR HOMELAND SECURITY, *supra* note 50, at 64 ("[W]e must carefully weigh the benefit of each homeland security endeavor and only allocate resources where the benefit of reducing the risk is worth the amount of additional cost.").

449. *See* De Young & Gravley, *supra* note 24, at 147.

450. *See* TOXIC TERROR, *supra* note 11, at 267.

451. *See Interview With Matthew Meselson, supra* note 227, at 108 ([W]hen you have a norm, a standard of behavior almost universally observed, if it gets broken anywhere, then there is a hazard that it could spread"); *see also* Bacevich, *supra* note 72, at 232 ("[A] resourceful terrorist would find ways to overcome [practical challenges]. . .").

B. *Do Other Environmental Laws Already Adequately Protect Us?*

Although viable threats to drinking water infrastructure exist, "a new mechanism" to deal with them may not have been necessary.[452] We may have ". . .simply need[ed] to build on what we have."[453] Many drinking water treatment facilities are already subject to emergency planning requirements under existing laws, such as the Clean Air Act ("CAA") and Emergency Planning and Community Right-to-Know Act ("EPCRA").[454] These emergency planning requirements resemble those now imposed by the SDWA Amendments. Furthermore, a variety of provisions under other existing laws could be used to prosecute the attempted contamination or disruption of drinking water systems.[455] The SDWA Amendments may therefore have simply added an expensive and unnecessary regulatory burden upon drinking water facilities.

Concern over potentially superfluous requirements is not solely based on economics. Additional layers of regulation can hinder compliance with existing requirements. Thus, duplicative regulatory requirements may inadvertently frustrate efforts to successfully address drinking water infrastructure security threats.[456] Accordingly, the similarities between the focus and requirements of the SDWA Amendments and existing environmental laws must be examined.

---

452. *See* Sokolski, *supra* note 98, at 217.

453. *See id.* (quoting former Virginia Governor James Gilmore and discussing this country's existing force of over two million first-responders and "massive health care system").

454. *See* Clean Air Act, 42 U.S.C. §§ 7401-7671 (2006), Emergency Planning and Community Right-to-Know Act, 42 U.S.C. §§ 11001-11050 (2006); *see also* ARNOLD W. REITZE, JR., AIR POLLUTION CONTROL LAW: COMPLIANCE AND ENFORCEMENT 164 (2001) (explaining that drinking water treatment plants and POTWs are often subject to CAA § 112(r)).

455. *See* Kornfeld, *supra* note 2, at 472-77 (discussing a host of statutes, including the Biological Weapons Anti-Terrorism Act of 1989, the Anti-Terrorism and Effective Death Penalty Act of 1986, Acts of Terrorism Transcending National Boundaries, and USA PATRIOT Act of 2001, aimed specifically at prosecuting terrorists for such things as ". . .hacking into computers, chemical and nuclear weapon use, and aiding or supporting terrorists").

456. *See* J.B Ruhl et al., *Environmental Compliance: Another Integrity Crisis or Too Many Rules*, 17 WTR NAT. RESOURCES & ENV'T 24, 27 (2002) ([W]hen it comes to compliance with environmental requirements, "the most important factor by far [is] the sheer number of regulations. . .").

1. Existing Emergency Planning Requirements

Under CAA § 112(r) and EPCRA, many drinking water treatment facilities are already required to prepare emergency response plans for releases of hazardous substances and implement programs to prevent such releases.[457] The SDWA Amendments overlap these emergency planning requirements for one of the likelier consequences of a drinking water infrastructure attack – the release of hazardous chemicals often stored at drinking water treatment facilities.[458] Although EPCRA and CAA § 112(r) focus upon *accidental* releases of hazardous substances, response planning considerations for such *intentional* releases are virtually identical.[459] Consequently, the SDWA Amendments' emergency planning provisions are redundant to existing response requirements, at least with respect to this specific threat. Nevertheless, despite this overlap, CAA§ 112(r) and EPCRA are insufficient to independently address the unique vulnerabilities of drinking water infrastructure components and the range of threats posed to them by terrorism.[460]

a. CAA § 112(r)

CAA § 112(r) ". . .created the first significant federal program to focus on the prevention of accidental catastrophic environmental releases of hazardous pollutants."[461] There are three major elements of Section 112(r)'s program: (1) identifying hazards that may result from releases of extremely hazardous substances; (2) designing and maintaining a safe facility, free from accidental releases; and (3) minimizing the consequences of accidental releases that nevertheless occur.[462] Facilities regulated under the CAA as stationary sources of air pollutants are subject to Section 112(r) if certain hazardous substances are present at the facility in an amount greater than established threshold quantities.[463] Chlorine and ammonia, substances frequently present at or used

457. *See* REITZE, *supra* note 454, at 164 (explaining that drinking water treatment plants and POTWs are often subject to CAA § 112(r)).

458. *See* 42 U.S.C. § 300i-2(a)(1) (2006) (vulnerability assessments must address the use, storage, and handling of chemicals); *see also id.* at § 300i-2(b) (addressing ERP requirements).

459. *See* Beth A. Henning, *EPCRA Emergency Plans: What to Consider Post-September 11*, 16 WTR NAT. RESOURCES & ENV'T 172, 174 (2002).

460. *See* Copeland & Cody, *supra* note 3, at 3.

461. REITZE, *supra* note 454, at 161.

462. *See id.*; *see also* 42 U.S.C. § 112(r)(1) (2006) (the "general duty" clause).

463. *See* 42 U.S.C. § 112(r)(7)(B)(ii) (2006).

by drinking water treatment facilities, are both specifically regulated pursuant to Section 112(r)(3).[464] Consequently, many drinking water facilities are regulated under CAA § 112(r).[465]

Owners or operators of facilities regulated under CAA § 112(r) must prepare a "risk management plan" ("RMP") addressing the hazards identified for each listed substance present at the facility.[466] RMP's are designed to detect and prevent or minimize accidental releases of listed substances.[467] Similar to the SDWA Amendments' ERPs, CAA RMPs also are required to dictate steps for a prompt emergency response to such releases.[468] RMPs must include: " . . .an estimate of potential release quantities, downwind effects (known as an "offsite consequence analysis"), [and] population exposure. . ."[469] The SDWA Amendments' legislative history indicates that the RMPs' focus on accident prevention goes beyond the SDWA Amendments and EPCRA's strictly response-oriented emergency plans.[470] Furthermore, unlike SDWA Amendment ERPs, RMPs must be updated every five years, anytime an additional regulated substance is present at the facility in an amount above the threshold quantity, or if EPA regulates a new substance.[471]

b. EPCRA

EPCRA's emergency planning provisions ". . .are designed to promote the discovery and mitigation of risks associated with chemical use in the community."[472] As EPCRA's requirements apply to more facilities than just stationary sources of air pollutants, its coverage is broader than CAA § 112(r). However, similar to CAA § 112(r), EPCRA's requirements are triggered if a listed extremely hazardous substance ("EHS") is present at a fa-

464. *See* 42 U.S.C. § 112(r)(3) (2006).

465. *See* REITZE, *supra* note 454, at 163 ("The chemicals most likely to require a § 112(r) response include chlorine, because of its low threshold and its common use in water and wastewater treatment.").

466. *See id.* at 161; *see also* 42 U.S.C. § 7412(r)(7(B)(ii) (2006).

467. *See* 42 U.S.C. § 112(r)(7)(B)(ii) (2006).

468. *See id.*

469. *See* Joseph A. Siegel, *Terrorism and Environmental Law: Chemical Facility Site Security vs. Right-To-Know?*, 9 WIDENER L. SYMP. J. 339, 352 (2003).

470. *See* 147 Cong. Rec. E2410, *supra* note 240 (statement of Rep. Gillmor explaining that the SDWA Amendments do not require drinking water systems ". . .to determine the consequences of intentional acts or terrorist acts, analyze their use of specific chemicals, including chlorine, as opposed to other chemicals, or to characterize the risk of any offsite impact").

471. *See* 40 C.F.R. § 68.190.

472. Henning, *supra* note 457, at 173.

cility in an amount exceeding its threshold planning quantity ("TPQ").[473] Because EPCRA's TPQs for chlorine and ammonia are relatively low, many drinking water facilities are subject to EPCRA's emergency planning requirements in addition to those under CAA § 112(r).[474]

EPCRA requires local emergency planning committees ("LEPCs") to create comprehensive emergency response plans for any regulated facility within their emergency planning district.[475] Similar to SDWA Amendment ERPs, EPCRA emergency response plans include, among other information, procedures to be followed by emergency personnel and facility owners in the event a listed EHS is released into the environment.[476] Furthermore, "[i]n developing and updating emergency plans, LEPCs utilize a 'hazards analysis' – a three step decisionmaking process which identifies the potential hazards facing a community with respect to accidental releases of EHSs and other hazardous chemicals."[477] Both vulnerability and risk analyses are steps of this decisionmaking process.[478]

EPCRA and CAA § 112(r)'s emergency planning requirements mirror those of the SDWA Amendments with respect to how releases of hazardous substances are addressed. The similarities are well-recognized. The SDWA Amendments' legislative history discusses the possibility that its new requirements could lead to a ". . .duplication of effort. . ." under EPCRA.[479] To minimize this potential, drinking water facilities are required to certify that they have coordinated, to the extent possible, with

473. *See* 42 U.S.C. § 11002(b)(1) (2006); *see also id.* at § 11002(b)(2) (a governor or state emergency response commission may designate additional facilities subject to EPCRA's planning requirements).

474. *See* 40 C.F.R. § 355, Appdx. A (listing a TPQ of 100 pounds for chlorine and 500 pounds for ammonia).

475. *See* 42 U.S.C. § 11003(a) (2006).

476. *See* 42 U.S.C. § 11003(c)(2) (2006); *see also id.* at § 11049(8) (defining "release").

477. Henning, *supra* note 457, at 173; *see also* Trang T. Tran, *The Emergency Planning and Community Right-To-Know Act and National Security: Restricting Public Access To Location Information of Hazardous Chemicals*, 8 ENVT'L LAW 369, 373 (2002) (discussing the requirements of 42 U.S.C. § 11003(c)(5) – (7)).

478. *See* Henning, *supra* note 457, at 173.

479. *See* 147 Cong. Rec. E2410, *supra* note 240 (statement of Rep. Gillmor) (recognizing that drinking water systems must coordinate with LEPCs while preparing ERPs ". . .for the purposes of avoiding duplication of effort and taking advantage of previous information developed by LEPCs for first responders. . .").

LEPCs under EPCRA when preparing or revising their ERPs.[480] Apparently recognizing a relationship between CAA § 112(r) RMPs and EPCRA ERPs, EPA also encourages LEPCs to incorporate RMPs into EPCRA ERPs.[481]

2. CAA § 112(r) and EPCRA Do Not Adequately Protect Drinking Water Infrastructure

Despite certain overlapping requirements, EPCRA and CAA § 112(r) are not sufficiently tailored to drinking water systems to independently address emergency situations at such facilities. Indeed, EPCRA and CAA § 112(r)'s emergency planning requirements have existed for years, yet the use of chlorine and other hazardous substances at water treatment facilities still poses a risk to millions of people.[482] There are several reasons why EPCRA and CAA § 112(r) are insufficient to address drinking water infrastructure security threats.

EPRCA and CAA § 112(r)'s focus on releases of individual hazardous chemicals is simply too narrow to provide the kind of comprehensive system-wide risk assessment and response planning needed to secure drinking water infrastructure networks from terrorist attack. First and foremost, scenarios involving intentional contamination, disruption, and most certainly, cyber attacks on drinking water infrastructure components are beyond the scope of EPCRA and the CAA § 112(r). These events simply are not contemplated within EPCRA and the CAA § 112(r)'s focus on addressing accidental releases of hazardous chemicals.

Second, the drinking water contaminants likeliest to be used in an intentional attack are not "present" at drinking water facilities. Consequently, they do not trigger EPCRA or CAA § 112(r)'s requirements, and their release into drinking water supplies, intentional or otherwise, is left unaddressed.

The most vulnerable drinking water infrastructure components, storage and distribution systems, are not covered by the EPCRA or CAA § 112(r) emergency plans for similar reasons. Because EPCRA and CAA § 112(r) only address facilities at

480. *See* INSTRUCTIONS TO ASSIST COMMUNITY WATER SYSTEMS IN Complying, *supra* note 232, at 10; *see also* 42 U.S.C. § 300i-2(b) (2006).

481. *See* Tran, *supra* note 477, at 373; *see also* 40 C.F.R. § 68.12(b)(3) (requiring facilities to ensure that ". . .response actions have been coordinated with local emergency planning and response agencies").

482. *See Chlorine Gas at Wastewater Plants Places 19 Million at Risk, Report Says*, 34 BNA ENV'T REP. 2704-05 (Dec. 12, 2003).

which sufficient quantities of regulated chemicals are stored, only main drinking water treatment plants will receive consideration in the emergency plans. Other infrastructure components where chemicals are not "present" will not be covered.

Lastly, unlike the SDWA Amendments' requirements, drinking water facilities can escape regulation under EPCRA and CAA § 112(r).[483] By simply switching to an unregulated alternative substance or reducing the amount of chlorine present below threshold planning quantities, drinking water facilities can avoid CAA § 112(r) and EPCRA's emergency planning requirements. Other types of facilities have dodged the CAA § 112(r)'s RMP requirements in this way.[484] Furthermore, even for those facilities subject to CAA § 112(r), emergency response plans and risk prevention programs are not uniformly required.[485] These facilities may nevertheless have sufficient quantities of hazardous substances present to threaten pubic health.[486] Thus, under EPCRA and CAA § 112(r), facilities that could pose an immediate danger to the public if attacked can avoid the very requirements that would make them safer.

Enforcing America's existing environmental laws has ". . .a distinct and vital role in the protection of the American homeland. . ."[487] The threat to public health posed by releases of chlorine and other hazardous substances from drinking water treatment facilities are adequately, and perhaps better, addressed by EPCRA and CAA § 112(r)'s risk prevention requirements. Indeed, some suggest that only slight amendments to EPCRA or the CAA would enable them to better address deliberate releases of hazardous substances caused by terrorist acts.[488] How-

483. *See* 42 U.S.C. §§ 300i-2(a)(1), 300i-2(b) (2006) (SDWA Amendments apply to all community water systems serving more than 3,300 people).

484. *See* REITZE, *supra* note 454, at 169 ("Many facilities changed their operations to avoid CAA §112(r) requirements by changing the chemicals used or by lowering the inventory below threshold amounts.").

485. *See id.* at 166-67 (discussing 40 C.F.R. § 68.90 (requiring ERPs for only Program II and III facilities) and 40 C.F.R. § 68.170 and § 68.175 (requiring prevention programs for Program II and III facilities)).

486. *See* Siegel, *supra* note 469, at 373 ("[A] one-ton cylinder of chlorine falls below the [RMP] thresholds. . .but can create levels of chlorine gas two miles off-site that are considered 'immediately dangerous to life and health").

487. Attorney General John Ashcroft, Prepared Remarks, Meet and Greet With Environmental Press (Mar. 11, 2003) ("Compliance with and enforcement of these laws makes real difference in our level of national preparedness").

488. *See* Henning, *supra* note 457, at 174 ("LEPCs can utilize these same [EPCRA] planning principles to update plans for consideration of *deliberate* releases caused by terrorist activity"); *see also* Sutton, *supra* note 213, at 153 (suggesting

ever, the chemical-specific focus of these laws is inadequate to address the range of terrorist threats to sprawling networks of drinking water infrastructure. There are currently ". . .too many seams in our current response plans and capabilities."[489] Consequently, the SDWA Amendments' planning requirements are necessary to address intentional threats to drinking water infrastructure security.

3. Contaminating or Disrupting Drinking Water Systems is Already Illegal

The SDWA Amendments' increased penalties for tampering with drinking water systems do little to substantively increase drinking water infrastructure security.[490] A variety of existing laws could be used to prosecute attempts to contaminate or disrupt drinking water supplies.[491] Federal criminal law already proscribes the creation, possession, and use of biological weapons.[492] The development, production, and use of chemical weapons is similarly criminalized.[493]

Existing environmental laws also already provide potential causes of action against the intentional contamination of drinking water. It is illegal under the Clean Water Act to ". . .discharge any radiological, chemical, or biological warfare agent. . .into the navigable waters."[494] Source waters used for drinking water supplies often will be navigable waters. Because the Clean Water Act is a strict liability statute and does not require that prohibited discharges be committed with "the intention of harming per-

---

amending EPCRA ". . .to include the preparation of plans. . . for bioterrorism prevention, preparedness, and response. . .").

489. NAT'L STRATEGY FOR HOMELAND SECURITY, *supra* note 50, at 42 (discussing various federal emergency response plans); *see also* Kristin Choo, *Controversial Cure: Proposed CDC Model Act on Bioterrorism Seeks to Clarify State Enforcement Powers*, 88 AMER. BAR. ASSOC. J. 20 (2002) (explaining that U.S. public health laws are insufficient to prepare us for today's terrorist threats).

490. *See* Public Health Security and Bioterrorism Preparedness and Response Act of 2002, *supra* note 6, at § 403(3), 116 Stat. 594, 687 (codified at 42 U.S.C. § 300i-1).

491. *See* Kornfeld, *supra* note 2, at 476-77 (discussing the use of the USA Patriot Act to prosecute attempts to hack into drinking water utilities' computer systems).

492. *See, e.g.*, Dagen, *supra* note 212, at 551-55 (discussing the Antiterrorism and Effective Death Penalty Act of 1996); *see also* Kellman, *supra* note 75, at 465-66.

493. *See* Webster, *supra* note 22, at 189 (discussing the Chemical Weapons Convention Implementation Act of 1998).

494. 33 U.S.C. § 1311(f) (2006).

sons," successfully prosecuting terrorists under this provision may be easier than under the SDWA's tampering provisions.[495]

The Resource Conservation and Recovery Act ("RCRA") offers another possibility for prosecuting such acts. Under RCRA, dumping hazardous wastes into navigable waters is illegal.[496] Most drinking water contaminants of concern will be considered "hazardous waste" because of the risk they pose to human health and the environment.[497]

Accordingly, there are a variety of environmental and general criminal laws that can be used to prosecute terrorists who seek to cause harm via drinking water. The SDWA Amendments' increased civil and criminal penalties do little to augment the deterring effect of these existing laws. And regardless, many fundamentalist terrorists have demonstrated that they are ". . .in a state of mind which makes them undeterrable."[498] ". . .[G]iven that their activities are already illegal in most jurisdictions in which they operate," it is naïve to think that increased penalties will prevent terrorists from targeting drinking water infrastructure components.[499] Thus, the SDWA Amendments' enhanced fines do little to make drinking water systems substantially safer.

VII.

ARE WE ADDRESSING THE LIKELY THREATS?

Despite the underlying fundamental issues discussed above, the question of whether the SDWA Amendments effectively protect our drinking water remains. Unfortunately, the likeliest threats to drinking water infrastructure security have yet to be sufficiently addressed by the SDWA Amendments. This deficiency is largely because EPA ". . .lacks the basic information needed to implement a strategy to secure U.S. water sup-

495. *Compare* 33 U.S.C. § 1311(f) *with* 42 U.S.C. § 300i-2(d)(1) (defining "tamper" to mean the introduction of a contaminant into a public water system "with the intention of harming persons").

496. *See* 42 U.S.C. § 6903(3) (2006) (defining "disposal" as "the discharge, deposit. . .dumping, spilling, leaking, or placing of any. . .hazardous waste into or on any land or water. . ."); *see also id.* at § 6928(d) & (g) (providing criminal and civil penalties for violations of RCRA).

497. *See* 42 U.S.C. § 6903(5) (2006) (defining "hazardous waste").

498. *Lake*, *supra* note 343, at 115 (penalties "cannot perfectly deter [terrorism], because again . . . existential terrorists simply want to lash out at a society they hate.").

499. Fidler, *supra* note 99, at 15 ("Experience with international criminal law. . .suggests that the deterrent effect of criminalizing certain state and individual behavior under international law is not great.").

plies. . ."[500] EPA's lack of regulatory authority to compel implementation of "necessary security enhancements" to address identified infrastructure vulnerabilities also greatly hinders progress under the SDWA Amendments.[501] Lastly, the SDWA Amendments fail to regulate entire categories of drinking water systems, leaving the significant populations served by them exposed to un-assessed risks.

These faults represent critical obstacles to the SDWA Amendments' success in improving drinking water infrastructure security. Consequently, several amendments must be made to the SDWA Amendments in order to supplement ongoing efforts. First, EPA must be required to develop and disseminate improved baseline information regarding the terrorist threats the SDWA Amendments were intended to address. The SDWA Amendments should then be amended to require periodic updates of vulnerability assessments and ERPs based upon EPA's revised baseline threat information. EPA should also be granted broader regulatory authority to require drinking water facilities to implement security enhancements for identified vulnerabilities. Finally, more drinking water systems should be made subject to the SDWA Amendments' requirements. These steps will pave the way for true improvements in drinking water infrastructure security.

A. *Critical threat information was not provided to drinking water utilities*

1. The Consequences of Inadequate Baseline Threat Information

The lynch-pin of the SDWA Amendments is EPA's duty to provide drinking water facilities with accurate baseline information regarding:

> . . .which kinds of terrorist attacks or other intentional acts are the probable threats to –
>
> (A) substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water; or
>
> (B) otherwise present significant public health concerns.[502]

500. Najor, *supra* note 158, at 2078-79.

501. *See Controlling Bioterror*, *supra* note 19, at 69.

502. 42 U.S.C. § 300i-2(a) (2006).

The quality of this baseline threat information directly impacts how effectively drinking water facilities can fulfill their primary responsibilities under the SDWA Amendments.

EPA published a "Baseline Threat Document" that presented "an overview of threats, methodologies, and strategies for the [community water system] to consider as it develops a [vulnerability assessment]."[503] However, information regarding the type of "post-9/11" threats the SDWA Amendments were intended to address was not included in this document.[504] This failure left the regulated community unable to conduct meaningful vulnerability assessments - the foundation for evaluating and improving drinking water security under the SDWA Amendments.[505] The impacts from this inadequate baseline threat information have cascaded throughout virtually every aspect of EPA's drinking water security program. Because of this breakdown in the SDWA Amendments, ". . .the public interest is not being served."[506]

a. Vulnerability Assessments and ERPs

Vulnerability assessments, and the ERPs based upon their results, are "threat-driven exercise[s]."[507] ". . .[T]he threat serves as the. . .benchmark against which vulnerabilities are assessed."[508] Without an accurate evaluation of current threat information from EPA, drinking water facilities are unable to ". . .adequately assess the specific shortcomings of our public water systems, much less implement protective measures. . ."[509]

"In the absence of credible threat information from EPA, water utility staff decided for themselves what threats to include in their vulnerability assessments."[510] The only threats realisti-

503. INSTRUCTIONS TO ASSIST COMMUNITY WATER SYSTEMS IN COMPLYING, *supra* note 232, at 11.

504. *See* Najor, *supra* note 158, at 2078-79; *see also* Harris, *supra* note 15, at 26 ("EPA did not provide adequate threat information.").

505. Harris, *supra* note 15, at 23 (explaining that "utilities use vulnerability assessments to help determine how well water systems detect security problems and stop or delay undesired events, as well as measure response capabilities.").

506. *See Controlling Bioterror*, *supra* note 19, at 37 (statement of Rep. Dingell).

507. Harris, *supra* note 15, at 26.

508. VULNERABILITY ASSESSMENT FACTSHEET, *supra* note 238 (explaining how vulnerability assessments are premised upon a "Design Basis Threat" (DBT)).

509. *Controlling Bioterror*, *supra* note 19, at 5 (comments of Representative Capps).

510. *See* Harris, *supra* note 15, at 26; *see also id.* at 6 (explaining that water utility managers were also left to discern which facility components vulnerability assessments should emphasize).

cally familiar enough to drinking water utilities ". . .were those they encountered before 9/11."[511] "Traditional" threats consequently became the "benchmark" drinking water utilities used in performing vulnerability assessments. As a result, many vulnerability assessments and ERPs ". . .emphasize traditional, less consequential, and less costly . . ." pre-September 11th threats, such as vandalism, natural disasters, and disgruntled employees.[512] The SDWA Amendments' major planning requirements therefore may not address the very threats to our security ". . .that motivated passage of the Bioterrorism Act."[513] Vandalism, natural disasters, and disgruntled employees are ". . . certainly not what we are talking about post-9/11."[514]

EPA disputes that it provided inadequate baseline threat information, explaining that ". . .when we put together the baseline threat document. . .we did emphasize terrorism and terrorist attacks."[515] In addition to other stakeholders, the intelligence and law enforcement communities were involved in ". . .identifying and defining risks to public health in relation to such attacks/acts."[516] Furthermore, the stakeholders involved in the development of the Baseline Threat Document believed that ". . .the design basis threat selection should be left to individual utilities to account for the uniqueness of each water system. . ."[517] Accordingly, EPA explains that the baseline information it provided was

511. *See id.* at 4-5, *reprinted in Controlling Bioterror*, *supra* note 15, at 25-26; *see also Controlling Bioterror*, *supra* note 19, at 61 (comments of Representative Stupak, explaining that ". . .limited threat information provided by EPA resulted in utilities subjectively designing their assessments around pre-9/11 threats").

512. *See* Harris, *supra* note 15, at 25-26; *see also Hearing on Creating the Homeland Security Department*, *supra* note 41, at 238 (explaining that the methodology used by many large municipal water systems to assess their vulnerabilities was developed before September 11th).

513. *See* Harris, *supra* note 15, at 25-26; *see also Controlling Bioterror*, *supra* note 19, at 62 (comments of Representative Stupak explaining that "[t]he reason why you had the Bioterrorism Act was because of 9/11 . . . .").

514. Harris, *supra* note 15, at 26 (comments of Representative Capps); *see also* Booth et al., *supra* note 213, at 1 (Plans "now must be developed to counteract the terrorist goal of creating as much death, suffering, and destruction as possible.").

515. *Controlling Bioterror*, *supra* note 19, at 62; (comments of Benjamin Grumbles); *see also id.* at 58 (explaining that "[i]t wasn't just [about] the pre 9/11 world, it was post 9/11").

516. Memorandum from G. Tracy Meehan, Assistant Administrator, Office of Water to Jeffrey K. Harris, Director for Program Evaluation, U.S. Envtl. Prot. Agency at 2 (June 16, 2003), *reprinted in Controlling Bioterror: Assessing Our Nation's Drinking Water Security Hearing Before the Subcomm. on Env't and Hazardous Materials of the House Comm. on Energy and Commerce*, 108th Cong. 30 (2004).

517. Harris, *supra* note 15, at 30-31 (explaining that an entire chapter of the Baseline Threat Document "focused heavily on consideration of the terrorist threat as

intended to simply provide a ". . .general description of the full range of threats."[518] Individual water utilities were responsible for seeking additional specific information to conduct vulnerability assessments from local law enforcements agencies on their own.[519]

Nevertheless, EPA acknowledges that developing up-to-date baseline threat information – exactly what the SDWA Amendments required in 2002 - is still ". . .an evolving effort. . ."[520] EPA concedes that aggregated information gleaned from completed vulnerability assessments ". . .*will* help us develop a baseline for water security. . ."[521] Research on drinking water threat assessment is similarly identified by EPA as a remaining "overarching need."[522] More than three years after EPA was to have disseminated baseline threat information, ". . .a database of all priority chemical, biological, biochemical, and radiological contaminants specific to water is. . .[still] not currently available."[523] EPA's Homeland Security Strategy also recognizes such critical information gaps.[524] Accordingly, EPA confirms that it has yet to develop sufficient baseline threat information, and this failure has adversely impacted the major prongs of the SDWA Amendments' approach to drinking water security.

b. Implementation of Security Enhancements

Without adequate threat data, the ability of drinking water facilities to implement appropriate security measures is im-

---

well as the national resources that are available to utilities to obtain threat information . . . .").

518. *Id.* at 3, *reprinted in Controlling Bioterror*, *supra* note 15, at 31.

519. *See id.*

520. *See* WATER SECURITY RESEARCH AND TECHNICAL SUPPORT ACTION PLAN, *supra* note 154, at 14.

521. Memorandum from G. Tracy Meehan, Assistant Administrator, Office of Water to Jeffrey K. Harris, Director for Program Evaluation, Cross-Media Issues, U.S. Envtl. Prot. Agency 2 (Aug. 22, 2003), *reprinted in Controlling Bioterror: Assessing Our Nation's Drinking Water Security Hearing Before the Subcomm. on Env't and Hazardous Materials of the House Comm. on Energy and Commerce*, 108th Cong. 15 (2004) (emphasis added).

522. *See* WATER SECURITY RESEARCH AND TECHNICAL SUPPORT ACTION PLAN, *supra* note 154, at 11-12; *see also id.* at 14-15 (describing research projects involving the "[i]dentification and prioritization of contaminant threat scenarios facing the drinking water sector . . ." and the "[d]evelopment of an improved understanding of the role of biologically-produced toxins as a drinking water contaminant.").

523. *See id.* at 15.

524. *See generally* U.S. ENV'T PROTECTION AGENCY, HOMELAND SECURITY STRATEGY 31 (2004) (discussing research and development activities to "advance the state of knowledge" in areas relevant to homeland security).

paired.[525] "The threats. . .selected for consideration during a vulnerability assessment will dictate, to a great extent, the risk reduction measures that should be designed to counter the threat(s)."[526] Vulnerability assessments based upon "traditional" non-terrorist threats therefore prevent water utilities from, ". . .justify[ing] the security upgrades necessary to defend against terrorism."[527] Accordingly, inaccurate baseline threat information may either discourage facilities from implementing appropriate security enhancements, or it may result in misguided and wasteful security measures that fail to address the most urgent vulnerabilities.

c. Response Actions

EPA's insufficient baseline threat information also diminishes the ability of drinking water facilities to effectively respond to potential threats.[528] Drinking water facilities often must decide how to respond to possible contamination threats in time frames as short as one hour.[529] Thus, accurate baseline threat information is integral to drinking water facilities' ability to assess whether a potential threat is viable, whether it warrants a response action, and how to properly focus a response action once initiated. Because such actions cost money and affect public confidence in their drinking water, utilities must have accurate baseline information to avoid triggering needless response actions.

d. Funding Decisions

Poor baseline threat information may also result in imprudent funding decisions by government. Funding allocations for drinking water security needs are often made ". . .on the basis of vulnerability assessment information."[530] As explained above, vulnerability assessments premised upon an inaccurate design basis threat may result in a distorted or incomplete understand-

525. *See* Harris, *supra* note 15, at 23.

526. VULNERABILITY ASSESSMENT FACTSHEET, *supra* note 238.

527. Harris, *supra* note 15, at 26; *cf.* Sokolski, *supra* note 98, at 219 (Security efforts should "avoid focusing on the most horrific scenarios at the expense of preparing for the most likely ones.").

528. *See* Frank Kaiser, *Broadband Toxicity Test Kits Help Utilities Respond to Security Threats*, WATERWORLD, July 2004, at 42.

529. *See* RESPONSE PROTOCOL TOOLBOX, MODULE 2, *supra* note 62, at 19; *see also id.* at 10 ("[T]here is a need to evaluate the credibility of any contamination threat and identify appropriate response actions in a very short period of time.").

530. EXPERTS' VIEWS ON HOW FEDERAL FUNDING CAN BEST BE SPENT TO IMPROVE SECURITY at 10, *reprinted in Controlling* Bioterror, *supra* note 137, at 50.

ing of infrastructure vulnerability. Such misguided vulnerability assessments may therefore lead to scant infrastructure funding being diverted away from more significant security needs.

e. Drinking Water Security Program Performance Goals

Finally, because EPA lacks adequate basic threat information, it has been unable to ". . . develop specific measurable performance indicators of water security activities. . ."[531] In other words, because EPA does not yet understand which threats to drinking water security are the most likely, ". . .EPA cannot determine whether its strategy has resulted in improved water security."[532] Perhaps more problematic, EPA similarly cannot tell where its strategy has failed. Thus, EPA's inadequate baseline threat information fundamentally impairs efforts to protect drinking water infrastructure at virtually every programmatic stage.

2. Requiring updates under the SDWA Amendments

a. Updating Baseline Threat Information

The SDWA Amendments currently do not require EPA to update the baseline threat information it provided to drinking water utilities.[533] Because terrorism is an "ever-changing" threat and for all the reasons discussed above, it is "critically important" that the SDWA Amendments be amended.[534] EPA must be required under the SDWA Amendments to periodically revise its baseline threat document. EPA must then be required to disseminate this revised threat information to drinking water utilities. This amendment will ensure that drinking water facilities

531. Memorandum from Nikki L. Tinsley, Inspector General, U.S. Envtl. Prot. Agency to G. Tracy Meehan, Assistant Administrator, Office of Water 1 (Sept. 11, 2003), *reprinted in Controlling Bioterror: Assessing Our Nation's Drinking Water Security Hearing Before the Subcomm. on Env't and Hazardous Materials of the House Comm. on Energy and Commerce*, 108th Cong. 7 (2004); *cf.* HOMELAND SECURITY STRATEGY, *supra* note 522, at 2 (making the development of "key indicators to clearly measure water security results and achievements" a goal by the end of Fiscal Year 2005).

532. Memorandum from Nikki L. Tinsley, at 5, *reprinted in Controlling* Bioterror, *supra* note 529, at 11 (". . .EPA cannot monitor program performance against goals").

533. *See also* Chilakamarri, *supra* note 18, at 935 (explaining that sections 1434 and 1435 ". . .do not require or allow the Administrator to put to use what may be learned from additional studies" regarding the potential threats to our nation's drinking water supply).

534. *See* NAT'L STRATEGY FOR HOMELAND SECURITY, *supra* note 50, at 4; *see also Controlling Bioterror*, *supra* note 19, at 38 (comments of Benjamin Grumbles, EPA Assistant Administrator for Water).

have proper information regarding the probable drinking water threats the SDWA Amendments were intended to address so that they can ". . .adequately protect against terrorist attacks. . ."[535]

EPA's revised baseline threat information should include a minimum threat level, based on current terrorist threats, against which utilities can meaningfully assess their vulnerabilities.[536] Threat determinations cannot be left ". . .open to interpretation. . ." by individual utilities.[537] Similarly, EPA should provide "clear guidance" on what facility components utility managers should focus on in conducting vulnerability assessments.[538] This supplemented information will provide both utilities and EPA with the foundation needed to make better decisions regarding drinking water infrastructure security.

However, responsibility for providing improved baseline threat information does not lie with EPA alone. The Department of Homeland Security ("DHS") is charged with facilitating the sharing of homeland security information ". . .relevant to threats and vulnerabilities in national critical infrastructure. . ."[539] Problems coordinating the sharing of such information between DHS and EPA limits EPA's ability to provide the regulated community with critical data. Thus, DHS must also increase its efforts to share timely infrastructure threat information with EPA.

b. Updating Vulnerability Assessments and ERPs

The SDWA Amendments should also be amended to require periodic updates of vulnerability assessments and ERPs based upon current baseline threat information ". . .or if there is a ma-

535. *Utilities Need More Security Information To Guard Against Terrorism*, *supra* note 331, at 331 (discussing a finding that drinking water utilities need more information of threats to drinking water infrastructure).

536. *See* Letter from Nikki Tinsley, Inspector General, U.S. Envtl. Prot. Agency to Representative Paul E. Gillmor, Chairman, House Subcommittee on Environment and Hazardous Materials, *reprinted in Controlling Bioterror: Assessing Our Nation's Drinking Water Security, Hearing Before the Subcomm. on Env't and Hazardous Materials of the House Comm. on Energy and Commerce*, 108th Cong. 79 (2004).

537. *See id.*

538. *See* Harris, *supra* note 15, at 27.

539. Press Release, *supra* note 207, at ¶28; *see also* Memorandum from Nikki L. Tinsley, at 6, *reprinted in Controlling Bioterror*, *supra* note 529, at 12 ("The National Strategy places responsibility with DHS for gathering threat and vulnerability information").

jor change to [a] water utility system configuration."[540] There is "great value" in requiring that such documents be ". . .revisited and revised and updated and adapted. . ."[541] EPA repeatedly acknowledges that, because protecting the nation's water infrastructure security "is a highly dynamic and evolving arena," vulnerability assessments must be "an iterative activity that water systems will have to review and update on a regular basis."[542] Both prior federal critical infrastructure security efforts[543] and other environmental laws[544] similarly recognize the importance of maintaining current vulnerability assessments and emergency planning measures.

Presently, however, vulnerability assessments and ERPs are only ". . .one-time requirements. . ." under the SDWA Amendments.[545] Thus, the SDWA Amendments lack a key requirement for all "active and effective" drinking water security programs.[546] If proper baseline threat information is eventually developed regarding existing threats to drinking water infrastructure, or new threats emerge, drinking water facilities are never required to incorporate such information into their security planning.[547] In addition, major changes to a water system's configuration will affect

---

540. *See* U.S. ENVT'L PROT. AGENCY, OFFICE OF WATER, LARGE WATER SYSTEM EMERGENCY RESPONSE PLAN: GUIDANCE TO ASSIST COMMUNITY WATER SYSTEMS IN COMPLYING WITH THE PUBLIC HEALTH SECURITY AND BIOTERRORISM PREPAREDNESS AND RESPONSE ACT OF 2002 2 (July 2003).

541. *Controlling Bioterror*, *supra* note 19, at 39 (comments of Benjamin Grumbles).

542. Harris, *supra* note 15, at 31; *see also Controlling Bioterror*, *supra* note 19, at 44, 62, 74.

543. *See White Paper*, *supra* note 195, at 3 (stating that "[f]requent assessments shall be made of our critical infrastructure's existing reliability, vulnerability and threat environment because, as technology and the nature of the threats to our critical infrastructures will continue to change rapidly, so must our protective measures and responses be robustly adaptive.").

544. *See* 42 U.S.C. § 11003(a) (2006) (requiring annual ERP review under EPCRA); *see also* 40 CFR 68.190 (requiring updates of RMPs under the CAA for various reasons, including the listing of a new hazardous substance or changes in a facility's operations).

545. *See* ADDENDUM TO THE *Instructions to Assist Community Water Systems in Complying*, *supra* note 241, at 3; *see also* 147 Cong. Rec. E2410, *supra* note 240 (statement of Rep. Gillmor) (The SDWA Amendments are "explicitly drafted not to . . . require systems that have completed vulnerability assessments to undertake another such assessment.").

546. *See* WATER SECURITY WORKING GROUP FINDINGS, *supra* note 30, at ii.

547. Patricia Ware, *Utilities Have Assessed Possible Threats; Measures Must Be Put in Place, EPA Says*, 35 BNA ENV'T REP. 2113-14 (Oct. 8, 2004) ("One challenge in ensuring water security is that the Bioterrorism Act does not require utilities to update their assessments and emergency response plans. . .").

the nature of its vulnerabilities. Over time, without periodic updates, vulnerability assessments and ERPs will therefore lose their relevance and utility. Accordingly, the SDWA Amendments must be amended to require that vulnerability assessments and ERP's be maintained as "living" documents so that they remain focused on addressing the most relevant threats to drinking water infrastructure security.[548]

B. *The SDWA Amendments Must Require Security Upgrades*

Currently, EPA does not have authority to ensure that adequate steps are being taken to protect the nation's critical drinking water infrastructure. While many drinking water utilities have voluntarily taken steps to resolve vulnerabilities identified in their facility assessments, they are under no statutory obligation to do so.[549] EPA also has no regulatory authority to otherwise require repairs, upgrades, personnel training, or similar enhanced security measures to correct known drinking water infrastructure vulnerabilities.[550] Because failing to address such vulnerabilities is not a SDWA violation, the SDWA's enforcement and citizen suit provisions are useless to compel such improvements at drinking water facilities.[551] Requiring enhanced security measures is critical to the security of drinking water systems as they serve to deter would-be attackers, increase detection and response capabilities, and limit the potential impacts of a successful attack.[552]

---

548. *See, e.g.*, WATER SECURITY WORKING GROUP FINDINGS, *supra* note 30, at iv (vulnerability assessments and ERPs must be kept "up-to-date as 'living' documents."); *see also* LARGE WATER SYSTEM EMERGENCY RESPONSE PLAN OUTLINE, *supra* note 538, at 2 ("It is important to note that the Water System ERP is a "living" document requiring periodic updates . . . .").

549. *See* Chilakamarri, *supra* note 18, at 934 (The SDWA Amendments do not ". . .empower the EPA to require any additional. . .action by the [community water systems] to protect their water supplies"); *see also* Ware, *supra* note 545, at 2113-14.

550. *See* Chilakamarri, *supra* note 18, at 935; *see also Controlling Bioterror*, *supra* note 19, at 70 (comments of Benjamin Grumbles describing that EPA's role under the SDWA Amendments is limited to providing tools, training, and assistance to help utilities ". . .carry out their plans as they develop them").

551. *See* Chilakamarri, *supra* note 18, at 938-39 (explaining that "SDWA section 1414 only provides the EPA with enforcement authority over SDWA violators. It does not provide the EPA with the power proactively to protect water systems when no statutory violation has occurred."); *see also id.* ("[S]ection 1449 suffers the same weakness . . . because citizen suits can only be initiated when actual violations of the SDWA or its regulations have occurred.").

552. *See* RESPONSE PROTOCOL TOOLBOX, MODULE 1, *supra* note 36, at 23 ("[E]nhancements to the physical security of distribution system elements . . . may deter the attack itself.").

Accordingly, drinking water facilities should be required under the SDWA Amendments to address identified infrastructure vulnerabilities by implementing "best security practices."[553] This standard should then be made an "applicable requirement" under SDWA section 1414(i)(1).[554] EPA will then be able to issue administrative orders and bring civil actions to require compliance with this standard pursuant to its existing enforcement authority under the SDWA.[555] Amending the SDWA Amendments to include a "best security practices" standard will provide EPA with true leverage to ensure a consistent level of security among drinking water facilities.

1. Vulnerability Assessments and ERP's Do Not Protect Drinking Water Infrastructure

Simply completing vulnerability assessments and ERPs ". . .does not equate to the outcome of reducing unacceptable security risks."[556] These documents are intended only to evaluate vulnerabilities to certain threats and develop responses to their potential consequences.[557] Vulnerability assessments and ERPs are therefore only the initial steps ". . .in what is a multi-step process to improving security."[558] "The next steps involve adopting security measures that both address vulnerabilities and mitigate the consequences of an attack."[559] However, as discussed, the SDWA Amendments presently ". . .[stop] short of ensuring that water systems or the EPA actively implement and enforce security mechanisms to prevent terrorist attacks."[560]

---

553. An EPA initiative is already underway to identify best security practices for drinking water facilities ". . .'since the water industry has very little standards for security.'" *See* Letter from Nikki Tinsley, *reprinted in Controlling Bioterror*, *supra* note 534, at 79.

554. *See* 42 U.S.C. § 300g-3(i)(1) (2006) (defining "applicable requirements" enforceable pursuant to SDWA § 1414).

555. *See* 42 U.S.C. § 300g-3(i)(a), (b), and (g) (discussing EPA's civil and administrative enforcement authorities).

556. *See* Ware, *supra* note 545, at 2113-14 (quoting Benjamin Grumbles, EPA Assistant Administrator for Water); *see also Controlling Bioterror*, *supra* note 19, at 11.

557. *See Controlling Bioterror*, *supra* note 19, at 5; *see also* Siegel, *supra* note 469, at 378 (explaining that ERPs are "flawed" because ". . .the plan to be certified only includes measures to respond to an attack or lessen the impact of an attack, rather than the site security measures to prevent an attack").

558. *Controlling Bioterror*, *supra* note 19, at 40.

559. *Id.*

560. Chilakamarri, *supra* note 18, at 935.

2. Voluntary Efforts Are Not Enough

"EPA's strategy for improving water security relies on water utilities to. . .institute security enhancements."[561] Unfortunately, this ". . .reliance on voluntary measures is likely to result in gaps in security. . ."[562] Such a framework ". . .presents the possibility for wide variation. . ." in whether or how even similarly designed drinking water facilities implement site security measures.[563] Without any government oversight or review of the implementation of security measures, the SDWA Amendments allows for ". . .weak prevention and response measures" at drinking water facilities.[564]

However, the drinking water industry is unlikely to support mandatory site security requirements. It favors voluntary efforts as being sufficient to ensure the security of the nation's drinking water supply.[565] The drinking water industry's reluctance is based partly upon a lingering fear that such requirements will stifle their ". . .flexibility to choose management options that will result in the best risk reduction opportunities."[566] Other critical infrastructure sectors have fought to keep themselves unburdened by mandatory security standards for similar reasons.[567] Consequently, requiring drinking water facilities to implement best security practices is a controversial proposal that likely will be resisted.[568]

---

561. *See* Harris, *supra* note 15, at 23; *see also* Ware, *supra* note 547, at 2113-14 (explaining that EPA has pursued "ways for utilities to voluntarily undertake security measures . . . .").

562. Siegel, *supra* note 469, at 368-69 (discussing post-September 11th security efforts at chemical plants).

563. *See id.* at 378.

564. *See id.*

565. *See Industry Releases Voluntary Guidelines To Improve Water System Monitoring*, 35 BNA ENV'T REP. 2587 (Dec. 17, 2004) (discussing voluntary security guidelines published by the Water Environment Federation).

566. Siegel, *supra* note 469, at 372; *see also* WATER SECURITY WORKING GROUP FINDINGS, *supra* note 30, at iii (explaining that "[a] rigid approach that requires a certain type of fence or other access control, or a prescribed information technology protection system or a standard set of personnel security policies would, automatically, over-address security needs for some utilities and under-address security needs for other utilities").

567. *See, e.g.*, John Mintz, *Bush Seeks Voluntary Chemical Plant Security Steps Criticized as Vulnerable to Terrorism, Industry Fighting Democratic Proposal for Mandatory Measures*, WASHINGTON POST, April 8, 2003, at A10 (discussing proposed legislation for chemical plants that emphasizes voluntary compliance with industry-developed security standards).

568. *See* Mark Scharfenaker, *Water Beat*, 96 AM. WATER WORKS ASSOC. JOURNAL 14-15 (Jan. 2004) (discussing opposition to proposed legislation requiring the

Clearly, drinking water utilities ". . .have strong incentives to protect their ability to provide safe and reliable water to their customers."[569] Indeed, many have acted without hesitation to implement effective measures to address vulnerabilities at their facilities. However, many of the most important security measures are very simple and commonly-used, such as denying unauthorized persons access to water supplies or facilities.[570] Furthermore, a "best security practices" standard, if implemented properly by EPA to account for facility-specific needs, will offer utilities the flexibility to choose suitable means to efficiently and effectively secure their facilities. Given the dire consequences of a successful attack on critical drinking water infrastructure, an enforceable standard requiring security measures is needed to assure the public that the necessary steps are being taken by water utilities to ensure their ability to provide a safe and reliable supply of drinking water.[571]

3. The Revised Imminent and Substantial Endangerment Provision Does Not Provide Authority to Require Site Security Measures

Revisions to the SDWA's imminent and substantial endangerment provision do not grant EPA sufficient authority to ensure public drinking water security.[572] Revised section 1431 expands EPA's preexisting substantial and imminent endangerment authority ". . .by allowing the EPA to act even when there is no actual 'contamination' of a water supply."[573] EPA can now take administrative or judicial action ". . .when there is a 'threatened

---

use of safer practices at chemical processing facilities); *see also* Siegel, *supra* note 469, at 371-72.

569. Letter from Christine Todd Whitman, Response to Question 3, *reprinted in Controlling Bioterror*, *supra* note 17 at 73; *see also* Steve Parascandola and J.P. Sevilla, *State incentive programs promote environmental stewardship*, TRENDS (Am. Bar Assoc. Section of Env't, Energy, and Natural Res., Chicago, IL.), Sept./Oct. 2005, at 13 ("[I]t often makes more sense to offer a carrot than use a stick.").

570. *See* ASSET BASED VULNERABILITY CHECKLIST, *supra* note 118, at 6-8 (describing security measures for wastewater treatment facilities, such as inspecting delivery vehicles, limiting access to infrastructure components, proper management of hazardous materials, that are equally applicable to drinking water utilities); *see also* EARLY WARNING MONITORING, *supra* note 32, at 9 (explaining that "[a] key line of defense is to prevent physical access by unauthorized persons to a free water surface, as in a reservoir").

571. *See Controlling Bioterror*, *supra* note 19, at 69 (comments of Rep. Stupak).

572. *See* Chilakamarri, *supra* note 18, at 938 (discussing amended SDWA section 1431).

573. *See id.* at 931-32.

or potential terrorist attack' that presents an imminent and substantial danger to public health."[574] Some argue that EPA's authority to issue corrective orders under the revised imminent and substantial endangerment provision could be construed broadly to require proactive steps to secure drinking water facilities.[575]

However, revised section 1431 was not intended to give EPA ". . .broad general authority. . ." to require the industry-wide action needed to address security concerns.[576] The SDWA Amendments' legislative history confirms that "[t]he authority granted to EPA in section 1431 is a *limited, case-by-case, contingent emergency power.*"[577] As explained, in determining whether to exercise these narrow emergency powers:

> EPA should not interpret 'potential terrorist attack' to mean that there is merely some possibility or statistical probability of a terrorist attack. Neither should EPA interpret a general warning, general announcement or general condition to be sufficient information of a threatened or potential terrorist attack. Specific, credible information is required, and all other elements of section 1431 must be met, including the existence of an imminent and substantial endangerment to the health of persons, that appropriate State and local authorities have not acted to protect the health of persons serves by the drinking water system, and that the EPA Administrator has consulted with State and local authorities. . .[578]

Thus, the revised imminent and substantial endangerment provision only was intended to respond to specific threats, or at most, to address vulnerabilities at individual utilities so glaring as to be characterized as an "emergency." It is therefore inadequate to require the necessary systematic improvements in security practices among the drinking water industry.

Maintaining the integrity of the nation's infrastructure is an ". . .enforcement priority. . ." for both EPA and the Justice De-

---

574. *See id.*; *see also* 42 U.S.C. § 300i (2006).

575. *See* Chilakamarri, *supra* note 18, at 944-47.

576. *See* Letter from Christine Todd Whitman, Response to Question 4, *reprinted in Controlling Bioterror*, *supra* note 17, at 73 (explaining EPA's understanding of its narrow authority under the amended imminent and substantial endangerment provision).

577. 147 Cong. Rec. E2410, *supra* note 240, at *2411 (statement of Rep. Gillmor) (emphasis added).

578. *Id.*; *cf.* Chilakamarri, *supra* note 18, at 936 ("It is not clear, however, whether or not the EPA may proactively protect the public by correcting vulnerabilities at PWSs without having any specific knowledge of an actual threat or attack upon the system").

partment.[579] However, at present, the SDWA Amendments simply do not provide the means to accomplish this goal. The SDWA Amendments' increased fines and jail time for tampering with drinking water systems are a 'smokescreen' compared to the true steps needed to ensure a safe and reliable supply of drinking water.[580] The implementation of site security measures to address known infrastructure vulnerabilities should be required under the SDWA Amendments, and EPA should be granted the authority to enforce compliance with this requirement. Strengthened accordingly, the SDWA Amendments will have the "teeth" necessary to ensure meaningful improvement in drinking water infrastructure security.[581]

C. *Gaps in the SDWA Amendments' Regulatory Coverage*

1. Unregulated Drinking Water Systems

The SDWA Amendments' requirements must apply to more drinking water systems. Millions of people are served on a daily basis by drinking water systems that are not subject to the SDWA Amendments' requirements.[582] These systems include those serving less than 3,300 people, non-community water systems, new drinking water systems constructed after the SDWA Amendments' effective date, and drinking water systems serving populations that will expand beyond 3,300 people.[583] The destruction or disruption of these systems ". . .could create local disaster or profoundly damage our Nation's morale or confidence."[584] Ironically, some of these unregulated and smaller

579. *See* Press Release, Department of Justice, Fact Sheet: Civil Environmental Enforcement Priorities 2 (March 11, 2003).

580. *See* Kellman, *supra* note 280, at 728 ("[D]eterrence is less effective in dealing with terrorists"); *see also* Public Health Security and Bioterrorism Preparedness and Response Act of 2002, *supra* note 6, at § 403(3), 116 Stat. 594, 687 (codified at 42 U.S.C. § 300i-1).

581. *See Controlling Bioterror*, *supra* note 19, at 2 (statement of Rep. Gillmor).

582. *See* Chilakamarri, *supra* note 18, at 932-33 (The SDWA Amendments ". . .exclude from coverage a significant portion of community water systems.").

583. *See id.*; *see also* U.S. ENVT'L PROT. AGENCY, WATER SECURITY STRATEGY FOR SYSTEMS SERVING POPULATIONS LESS THAN 100,000/15MGD OR LESS 3 (2002), *available at* http://www.epa.gov/safewater/security/index.html (illustrating that 45,503 community water systems serving between 25 and 3,300 people, 20,092 non-transient non-community water systems between 25 - 99,999, and 91,590 transient non-community water systems between 25 - 99,999 are unregulated by the SDWA Amendments).

584. NAT'L STRATEGY FOR HOMELAND SECURITY, *supra* note 50, at 30; *see also* Chilakamarri, *supra* note 18, at 927 ("Any attack on a public water system could be devastating . . . .").

drinking water systems are considered to be the most vulnerable to deliberate attack. They also receive the least funding to address security issues. If the SDWA Amendments are not amended to reach more of these unregulated systems, we remain susceptible to many of the ". . .same devastating effects. . ." attacks on larger drinking water systems could cause.[585]

Community water systems regulated under the SDWA Amendments serve over 240 million people - more than the majority of the country's population.[586] However, approximately 24 million people receive drinking water from community water systems not regulated by the SDWA Amendments.[587] In addition, "non-transient, non-community water systems" provide drinking water to almost 7 million people at universities, factories, and other locations with significant fixed populations.[588] "Transient, non-community water systems" regularly serve fluctuating populations of almost 13 million people at places such as highway rest stops, restaurants, national parks, and other tourist attractions such as the Kennedy Space Center.[589] These unregulated systems may provide terrorists with, at the very least, attractive symbolic or political value targets.[590] More of these unregulated systems must therefore be made subject to the SDWA Amendments, and a better plan to address their unique vulnerabilities should be developed.[591]

Aside from the sheer number of people receiving drinking water from systems not regulated by the SDWA Amendments, "[t]he most significant security issues in water supply are found

585. *See Oversight Hearings On Drinking Water System Security*, *supra* note 176.

586. *See* PROTECTING OUR WATER, *supra* note 12, at 4.

587. *See* U.S. ENVT'L PROT. AGENCY, FACTOIDS: DRINKING WATER AND GROUNDWATER STATISTICS FOR 2004 (2005), *available at* http://www.epa.gov/safewater/data/pdfs/data_factoids_2004.pdf.

588. *See* U.S. ENVT'L PROT. AGENCY, PROVIDING SAFE DRINKING WATER IN AMERICA: 2000 NATIONAL PUBLIC WATER SYSTEM COMPLIANCE REPORT 3 (2002), *available at* http://www.epa.gov/safewater/ars/annual/sdwcom2002.pdf; *see also* Chilakamarri, *supra* note 18, at 933.

589. *See* 2000 NATIONAL PUBLIC WATER SYSTEM COMPLIANCE REPORT, *supra* note 586, at 3; *see also* Chilakamarri, *supra* note 18, at 933.

590. *See* Chilakamarri, *supra* note 18, at 933.

591. *See* Sokolski, *supra* note 98, at 218-19 (discussing a pre-September 11th congressionally mandated advisory panel on domestic nuclear, chemical, and biological terrorism that ". . .criticized the government's emphasis on massive worst-case scenarios" because such a policy fails to optimize response capabilities for the more probable smaller-scale threats confronting the United States).

in small water systems, not large systems."[592] While problems at a large utility may put more people at risk, ". . .from a logistical point of view small water systems are the most vulnerable. . ."[593] "Large systems understand vulnerability assessment and security. . ."[594] "Smaller systems. . .generally lack the expertise and financial means to properly assess risks and implement security programs."[595]

Furthermore, the inherent obstacles to contaminating a large water supply are not as significant for smaller facilities.[596] Extensive treatment processes and barrier systems protecting larger systems are simply not feasible for smaller ones.[597] The protective effects of dilution are also diminished. Therefore, the likelihood of successfully contaminating or disrupting a smaller drinking water facility may be significantly greater than for a larger system. Moreover, such attacks come ". . .at much less risk to the perpetrators."[598]

Large drinking water systems are arguably ". . .the greatest targets of opportunity for terrorist attacks. . ."[599] However, an attack on a smaller drinking water system could have equally devastating consequences.[600] ". . .[A] terrorist might make a calculated decision to sicken or poison a cluster of small communities, thereby leaving public health officials to unravel a fatal or toxic puzzle."[601] "Even if just a small town or berg experienced an outbreak of [illness]. . .," the incident could easily cause mass-hysteria.[602] ". . .[S]uch attacks would indicate that there are no

592. *Oversight Hearings On Drinking Water System Security*, *supra* note 176; *see also* Copeland and Cody, *supra* note 3, at 2-3 ("[T]he more numerous smaller systems also tend to be less protected, and, thus, are potentially more vulnerable to attack. . .").

593. Kornfeld, *supra* note 2, at 483 ("Many complex issues plague small water systems that have little or no effect on large systems").

594. *Id.* at 451 (quoting *Oversight Hearings On Drinking Water System Security*, *supra* note 176).

595. *Id.*; *see also* PROTECTING OUR WATER, *supra* note 12, at 14 (explaining that staff for medium and smaller drinking water systems ". . .are forced to 'wear several hats'. . .[and are] less likely to have a dedicated security manager").

596. *See, e.g.*, Tucker & Sands, *supra* note 69, at 51 ("[A] small-scale attack on. . .a water tank would be more feasible"); *see also supra* Section VI(A)(3)(b).

597. *See* Kellman, *supra* note 75, at 443.

598. *Oversight Hearings On Drinking Water System Security*, *supra* note 176.

599. Copeland and Cody, *supra* note 3, at 2; *see also* Kornfeld, *supra* note 2, at 483 ("[A] large city strike may be more appealing to terrorists because of the publicity it would cause.").

600. *See Oversight Hearings On Drinking Water System Security*, *supra* note 176.

601. Kornfeld, *supra* note 2, at 468.

602. *Id.* at 471.

safe havens and thus, could have a major psychological impact on the public."[603] Accordingly, the consequences of a terrorist attack on a small drinking water system cannot be underestimated.

As required by the SDWA Amendments, EPA provided guidance to "very small" systems on how to conduct vulnerability assessments, prepare ERPs, and address threats to their ability to provide a safe supply of drinking water.[604] Furthermore, some states have enacted laws requiring vulnerability assessments and ERPs from drinking water facilities regardless of their size.[605] Thus, efforts are being made to address security at certain drinking water systems unregulated by the SDWA Amendments. The SDWA Amendments should nevertheless be amended to require uniform security measures among new and expanded drinking water systems, as well as at a greater number of smaller systems and non-community drinking water systems.

The tension between the need to focus on the security of larger utilities serving the greatest number of people and the fact that smaller systems are most in need of support illustrates the ". . .inherent dilemma. . ." in drinking water security.[606] By necessity, finite resources must be directed at the "highest priorities."[607] Assets, functions, and systems within the drinking water infrastructure sector ". . .are not equally important."[608] However, ". . .whatever does not receive attention becomes a more likely target."[609] Consequently, a comprehensive and consistent security strategy must be developed to ensure that the security needs

603. *Oversight Hearings On Drinking Water System Security*, *supra* note 176 (". . .[I]f several small water systems were contaminated with different unknown pathogens or contaminants, the impact on public health providers and government officials would be enormous. . ., many Americans. . .would question the safety of their water.").

604. *See* 42 U.S.C. § 300i-2(d) (2006); *see also* http://www.epa.gov/safewater/watersecurity/home.cfm?program_id=11 (providing self-assessment guidance for "very small" systems).

605. *See* Jackson, *supra* note 188, at 3 (discussing New York state law requiring vulnerability assessments and ERPs for all systems regardless of size).

606. *See* EXPERTS' VIEWS ON HOW FEDERAL FUNDING CAN BEST BE SPENT TO IMPROVE SECURITY at 10-11, *reprinted in Controlling* Bioterror, *supra* note 137, at 50.

607. *See* NAT'L STRATEGY FOR HOMELAND SECURITY, *supra* note 50, at 30; *see also* Press Release, Office of the Press Secretary, White House, December 17, 2003 Homeland Security Presidential Directive/HSPD-8: Subject: National Preparedness at ¶ 10 (December 17, 2003) *available at* http://www.whitehouse.gov/news/releases/2003/12/20031217-6.html; *see also* Press Release, *supra* note 207, at ¶ 32.

608. NAT'L STRATEGY FOR HOMELAND SECURITY, *supra* note 50, at 30.

609. EXPERTS' VIEWS ON HOW FEDERAL FUNDING CAN BEST BE SPENT TO IMPROVE SECURITY at 10, *reprinted in Controlling* Bioterror, *supra* note 137, at 50.

of unregulated drinking water systems receive proper attention and do not become an overlooked priority. Without question, this is an extraordinarily difficult task given the widely varying characteristics of such smaller systems.

2. Wastewater Treatment Plants?

The SDWA Amendments only regulate drinking water facilities. However, the integrity of wastewater infrastructure directly affects drinking water safety.[610] Furthermore, generally speaking, wastewater treatment plants suffer from many of the same vulnerabilities as drinking water facilities.[611] Nevertheless, there is no wastewater infrastructure security legislation comparable to the SDWA Amendments. Because of the absence of such legislation, the wastewater sector has not yet wholeheartedly ". . .follow[ed] the water industry's lead in embracing a cultural shift" regarding security.[612] Accordingly, wastewater infrastructure security legislation is needed to support drinking water security efforts.

Despite the absence of such legislation, the wastewater industry has taken steps to address certain security issues at their facilities.[613] Furthermore, EPA has attempted to bootstrap wastewater security along with its drinking water security efforts.[614] Guidance has been released regarding security measures at wastewater treatment plants.[615] Vulnerability assessment tools

610. *See Hearing on Homeland Security Funding on Behalf of The National Governors Association Before the Sen. Comm. on Appropriations*, 107th Cong. 410, at 22 (2002) (testimony of Michigan Gov. John Engler) (explaining that "[s]ignificant damage to [wastewater] infrastructure could result in loss of life, catastrophic environmental damage to rivers, lakes, and wetlands, contamination of drinking water supplies, long-term public health impacts, destruction of fish and shellfish production, and extreme disruption to commerce and the economy.").

611. *See* Shannon D. Spence and Wendelyn S. Stoveland, *The New Security Culture*, WATER ENVIRONMENT & TECHNOLOGY (Water Env't Fed'n, Alexandria, Virginia), Feb. 2004, at 4; *see also id.* at 3 (explaining that wastewater treatments systems may in fact be more readily accessible than drinking water systems because they ". . .are readily accessible to potential adversaries at nearly any sink or toilet").

612. *See id.* at 3 ("Security must become an integral part of all planning and decision-making processes.").

613. *See, e.g., Chlorine Gas at Wastewater Plants Places 19 Million at Risk, supra* note 480, at 2704-05 (explaining that "[m]ore than 20 million people who were once at risk from chemical releases at wastewater facilities are now safer because the facilities. . .have stopped using chlorine gas. . .").

614. *See* WATER SECURITY RESEARCH AND TECHNICAL SUPPORT ACTION PLAN, *supra* note 154, at 31 (describing projects to address the "overarching needs that apply to both drinking water and wastewater security and protection.").

615. *See generally* ASSET BASED VULNERABILITY CHECKLIST, *supra* note 118.

for wastewater facilities have been developed,[616] and funding has been provided for wastewater security training.[617] However, significantly less funding has been provided as compared to drinking water infrastructure security programs.[618]

A "Wastewater Treatment Works Security Act" similar in format to the SDWA Amendments was proposed in 2003, but failed to pass.[619] Therefore, comprehensive wastewater security legislation is still needed. Such legislation will not only help to further protect our drinking water, it will also safeguard another ". . .one of America's most valuable resources. . ."[620]

VIII.
ARE THE SDWA AMENDMENTS A FAILURE?

Although the SDWA Amendments should be strengthened to better protect the nation's critical drinking water infrastructure, they are far from a failure. The SDWA Amendments have brought about undeniable progress to the state of drinking water security. Awareness of drinking water infrastructure security issues has never been greater, and efforts to protect drinking water supplies have never been as focused. Because of the SDWA Amendments, ". . .we are smarter and safer as a country than we were 3 years ago."[621]

A. *The New "Culture of Security"*

One of the most important results of the SDWA Amendments is that water utilities are ". . .developing a never before seen cul-

616. *See Securing Small Wastewater Systems*, *available at*, http://www.nesc.wvu.edu/nsfc/SecuringWastewaterSystems.html (describing the American Metropolitan Sewerage Agency's VSAT software).

617. *See* EPA, Water Security, Grants and Funding, *available at* http://cfpub.epa.gov/safewater/watersecurity/financeassist.cfm (describing $1 million in funding to provide security training for small wastewater systems).

618. *See Sewer Lines at Wastewater Utilities Most Vulnerable to Attack, GAO Says*, 36 BNA ENV'T REP. 435 (Mar. 4, 2005) (explaining that since 2002, only $10 million have been spent to address wastewater security compared to over $200 million for drinking water security).

619. *See* Spence and Stoveland, *supra* note 611, at 3; *see also* Scharfenaker, *supra* note 568, at 14 (discussing other proposed wastewater security bills).

620. *See Securing Small Wastewater Systems*, *supra* note 616 (explaining that the nation's wastewater infrastructure is valued at more than $2 trillion).

621. *Controlling Bioterror*, *supra* note 19, at 38 (comments of Benjamin Grumbles, EPA Assistant Administrator for Water).

ture of security. . ."[622] This new "culture" is evident on an institutional scale from the growing number of organizations working on drinking water security issues, as well as the increasing number of publications addressing the subject.[623] It is also apparent at individual utilities. Facility staff are becoming sensitized to particular drinking water threats, and security measures are being incorporated throughout routine day-to-day operations.[624] As security considerations are now being designed into future drinking and wastewater infrastructure projects, this cultural shift represents a lasting change in how drinking water facilities operate.[625]

Creating this "culture of security" is an important development because it is one of the simplest yet most effective means to reduce threat potential and improve responsiveness.[626] Well-trained and vigilant employees improve early recognition, reporting, and response to potential threats.[627] In addition, incorporating safer designs and operating procedures ". . .during plant construction, upgrades, and major maintenance activities may be the most efficient way for utilities to, over time, improve security."[628] Accordingly, encouraging a culture of security sets the

622. PROTECTING OUR WATER, *supra* note 12, at 1; *see also id.* at 4 (Drinking water utilities are ". . .instilling a strong culture of security throughout the water community. . .").

623. *See, e.g.*, http://www.asdwa.org/security (the Association of State Drinking Water Administrators' website).

624. *See* PROTECTING OUR WATER, *supra* note 12, at 16 ("Everyone from the guard at the gate, to the receptionist, to the treatment plant operator must be aware that security is an important part of the job").

625. *See* WATER SECURITY RESEARCH AND TECHNICAL SUPPORT ACTION PLAN, *supra* note 154, at 36; *see also generally* Rufus Calhoun Young, Jr. and Dwight M. Merriam, *Homeland Security Begins At Home: Local Planning and Regulatory Review to Improve Security*, 55 LAND USE L. & ZONING DIGEST 11 (2003) (discussing the incorporation of homeland security factors into the land use review and approval process, as well as the design of various classes of facilities).

626. *See* WATER SECURITY WORKING GROUP FINDINGS, *supra* note 30, at vii ("Even when resources are limited, the simple act of increasing organizational attentiveness to security will reduce threat potential and increase responsiveness."); *see also* PROTECTING OUR WATER, *supra* note 12, at 16.

627. *See* RESPONSE PROTOCOL TOOLBOX, MODULE 2, *supra* note 62, at 27; *see also* RESPONSE PROTOCOL TOOLBOX, MODULE 1, *supra* note 36, at 23 ("The employees of a water utility are generally its most valuable asset in preparing for and responding to water contamination threats and incidents.").

628. WATER SECURITY WORKING GROUP FINDINGS, *supra* note 30, at iv (2005); *see also id.* at viii (consideration of security issues should be a factor in building plans and designs).

foundation for an enduring "active and effective security program."[629]

B. *Compliance with the SDWA Amendments*

The impressive compliance rates with the SDWA Amendments indicate that many drinking water systems have now gained significant insight into the strengths and weaknesses of their facilities.[630] "One hundred percent" of regulated drinking water systems serving populations of greater than 50,000 people completed the required vulnerability assessments and ERPs.[631] Most drinking water systems serving populations of greater than 3,300 people have done the same.[632] Despite legitimate concerns about the nature of the threats focused upon in initial vulnerability assessments, this increased awareness is a critical first step to improving security.

Moreover, as a result of the SDWA Amendments, most of the larger high-priority drinking water systems ". . .have begun or completed implementing security measures to address the vulnerabilities found in their VAs."[633] Increased precautions are now being taken to protect drinking water infrastructure.[634] For example, some drinking water utilities have addressed security concerns about storing chlorine gas onsite by switching to a ". . .more stable liquid form of chlorine instead of the more vulnerable compressed gas canisters that have traditionally been used."[635] Of course, these changes are not without their down-

629. *See id.* at ii; *see also* Steve Dennis, *Water Utility Security; What's in Store in 2004?*, 96 AM. WATER WORKS ASS'N J. 18 (Jan. 2004).

630. *See* Dennis, *supra* note 629, at 21 (In completing a vulnerability assessment ". . .you will learn more about the strengths and weaknesses of your system that you can ever imagine").

631. *See* Jack W. Moyer, *A Progress Report: Beyond VAs and ERPs: Things Local Water Systems Still Need and How State Drinking Water Administrators Can Help*, SEC. UPDATE (Ass'n of State Drinking Water Adm'rs, Washington D.C.), Summer 2005, at 2, *available at*, http://asdwa.citysoft.com/_uploads/documents/live/security news7-05.pdf.

632. *See id.*

633. *Id.*

634. *See* Kornfeld, *supra* note 2, at 452-58 (discussing security measures taken by various drinking water systems and regulator agencies post-September 11th); *see also Controlling Bioterror*, *supra* note 19, at 4 (discussing Los Angeles' post-September 11th security responses).

635. EXPERTS' VIEWS ON HOW FEDERAL FUNDING CAN BEST BE SPENT TO IMPROVE SECURITY at 9, *reprinted in Controlling* Bioterror, *supra* note 137, at 52; *see also* Kornfeld, *supra* note 1, at 448 (describing the removal of onsite chlorine tanks from Washington D.C.'s water utility).

sides.[636] While urgent vulnerabilities remain, the SDWA Amendments have spurred unparalleled efforts to improve drinking water infrastructure security.[637]

C. *Increased Research and Development*

Since the SDWA Amendments took effect, EPA has actively advanced the state of water security knowledge and technology. To address the SDWA Amendments' research requirements, EPA created a comprehensive water security research agenda: the *Water Security Research and Technical Support Action Plan*.[638] EPA's *Action Plan* ". . .describes the research and technologies needed to better address drinking water supply, water treatment, finished water storage, and drinking water distribution system vulnerabilities."[639] It ". . .identifies critical research and technical support projects in the areas of physical and cyber infrastructure protection; contaminant identification; monitoring and analysis; treatment, decontamination, and disposal; contingency planning; infrastructure interdependencies; and risk assessment and communication."[640] This research is greatly needed by the regulated community and regulators alike.[641]

There are now dozens of ongoing water security research projects.[642] Research is underway to improve the understanding of drinking water threats, and to determine the effectiveness of treatment and disinfection technologies.[643] New models are be-

636. *See* Letter from Christine Todd Whitman, *reprinted in Controlling Bioterror*, *supra* note 17, at 72 (explaining that disinfection alternatives such as ozone and ultraviolet light ". . .do not provide the necessary disinfection residual required for public health protection in the distribution system."); *see also Chlorine Gas at Wastewater Plants Places 19 Million at Risk*, *supra* note 480, at 2704-05 (explaining that the alternatives chemicals some plants have switched to are ". . .not safer than chlorine gas. . .").

637. *See* Ware, *supra* note 144, at 127 (describing lingering vulnerabilities in drinking water utility SCADA systems).

638. *See* 42 U.S.C. §§ 300i-3, 300i-4 (2006); *see also generally* WATER SECURITY RESEARCH AND TECHNICAL SUPPORT ACTION PLAN, *supra* note 154.

639. *Controlling Bioterror*, *supra* note 19, at 42.

640. WATER SECURITY RESEARCH AND TECHNICAL SUPPORT ACTION PLAN, *supra* note 154, at iii; *see also id.* at 3.

641. *See Utilities Need More Security Information To Guard Against Terrorism*, *supra* note 331, at 331; *see also supra* Section VII(A)(2)(a).

642. *See* Phibbs, *supra* note 115, at 1117-18 (discussing nearly a dozen homeland security research projects between EPA and the Army "to improve the detection and decontamination of chemical warfare agents and toxins that could be added to drinking water systems . . . .").

643. *See* Phibbs, *supra* note 332, at 231 (describing ongoing research regarding the ability of certain toxins to contaminate drinking water, the effectiveness of disinfec-

ing tested for predicting the fate and transport of contaminants in both source water and drinking water system components.[644] A set of standard analytical test methods to detect potential drinking water contaminants has been developed.[645] In addition, although initiated in response to HSPD-9, an "early-warning system" is in the works that may be especially useful to monitor for drinking water contamination.[646]

Other tools have been created to improve the dissemination of drinking water security information as it is developed. These avenues for exchanging information are vital to alerting drinking water utilities to emerging threats. For example, utilities, law enforcement and intelligence communities, and regulatory agencies can access and contribute to the Water Information Sharing and Analysis Center ("ISAC").[647] The Water ISAC is secure internet portal providing a ". . .comprehensive compilation of threat information and current research and intelligence on water security measures. . ."[648] In addition, drinking water utilities can now sign-up for the Water Security Channel - an email-based drinking water threat notification service.[649]

As a result of the SDWA Amendments' research requirements, information and tools to address drinking water infrastructure vulnerabilities ". . .are continually being developed and implemented."[650] These accomplishments offer the promise of

---

tion techniques, the ability to provide alternative supplies of drinking water, and contaminant detection methods).

644. *See* Memorandum from G. Tracy Meehan, at Attachment 1, *reprinted in Controlling Bioterror*, *supra* note 519, at 16; *see also* Phibbs, *supra* note 115, at 1117-18 (describing a "Water Test Loop" model developed to simulate a drinking water distribution system).

645. *See, e.g.*, Press Release: *EPA Researchers Lead Team to Select Standards for Analyzing Threatening Contaminants* (July 2, 2004), *available at*, http://www.epa.gov/ordnhsrc/news/news070204.htm (discussing the publication of ". . .a list of Standardized Analytical Methods (SAM) to be used by environmental laboratories in analyzing biological and chemical samples associated with threats to homeland security"); *see also Three New Detection Methods Approved For Monitoring Uranium in Drinking Water*, 35 BNA ENV'T REP. 1828-29 (Aug. 27, 2004).

646. *See* Patricia Ware, *New Drinking Water Security Initiatives Funded at $44Million in FY 2006 Request*, 36 BNA ENV'T REP. 378-79 (Jan. 21, 2005) (describing EPA's Water Sentinel Program).

647. *See Hearing on Creating the Homeland Security Department*, *supra* note 41, at 240-41 (2002) (statement of John P. Sullivan).

648. *See* Booth et al., *supra* note 215, at 7; *see also* PROTECTING OUR WATER, *supra* note 12, at 9-10.

649. *See* Patricia Ware, *Free Service to Provide Security Information To Water Utilities, State Agencies Launched*, 35 BNA ENV'T REP. 2401 (Nov. 19, 2004) (describing the Water Security Channel "WaterSC" service).

650. *See* Harris, *supra* note 15, at 32.

providing drinking water utilities the threat information needed to maintain up-to-date vulnerability assessments, the technology to address such vulnerabilities, and the ability to effectively respond in the event of an incident. Although much more research remains to be done, the SDWA Amendments have spurred significant advancement to the state of drinking water infrastructure security.[651]

D. *Training, Technical Assistance, and Funding*

Providing drinking water utilities with the tools, training, and technical assistance they need to become well-versed in infrastructure security is a "high priority" for EPA.[652] Training programs and guidance on everything from how to conduct thorough vulnerability assessments and ERPs to risk reduction practices have been offered by both EPA and other organizations.[653]

EPA's assistance has been an important factor in ensuring that drinking water utilities receive the training and support needed to comply with the SDWA Amendments. With the help of grants authorized under the SDWA Amendments, training programs are often available at little or no cost to facility operators.[654] Over $53 million in grants were awarded to large drinking water utilities to fund the development of vulnerability assessments and ERPs.[655] Various grants continue to be available from EPA and other government agencies to fund drinking water security training, technical assistance, and tool development.[656] Other means of funding individual drinking water infrastructure security

651. *See Controlling Bioterror*, *supra* note 19, at 64 (Facilities currently have no capacity for real-time monitoring of their distribution networks); *see also* EXPERTS' VIEWS ON HOW FEDERAL FUNDING CAN BEST BE SPENT TO IMPROVE SECURITY at 2, *reprinted in Controlling* Bioterror, *supra* note 137, at 47 (development of real-time monitoring should be high priority for receiving federal support).

652. *See Controlling Bioterror*, *supra* note 19, at 38 (comments of Benjamin Grumbles).

653. *See* Ware, *supra* note 646, at 378-79 (describing EPA's Water Alliance for Threat Reduction program to train utility operators at the highest risk system); *see also* http://cfpub.epa.gov/safewater/watersecurity/outreach.cfm (listing future and previously offered nationwide training courses, workshops, and drinking water security meetings).

654. *See* EPA, Water Security, Grants and Funding, *supra* note 617.

655. *See* Press Release, *Whitman Awards First Nationwide Water Security Grants as Part of $53 Million for Large Drinking Water Utilities* (June 7, 2002) *available at* http://yosemite.epa.gov/opa/admpress.nsf/30d624a93aeb27a18525701c005e42e4/c30e06aa1a5ac2e185256bd1005243aa!OpenDocument

656. *See* EPA, Water Security, Grants and Funding, *supra* note 617.

projects are available through both CWA and SDWA revolving loan funds.[657]

These grants are insufficient to fully fund the measures necessary to address drinking water infrastructure vulnerabilities. Consequently, utilities remain concerned about their ability to finance security improvements.[658] Nevertheless, the training and assistance offered to help drinking water utilities comply with the SDWA Amendments represents a significant initial investment toward improving drinking water infrastructure security.[659]

E. *Government Reorganization to Address Drinking Water Security*

Following September 11th, the mission of many government agencies was transformed to include drinking water infrastructure protection. In response, EPA and other such agencies restructured themselves to handle their new responsibilities. EPA created a specific Water Security Division ". . .to enhance the security of water and wastewater utilities and the ability to respond effectively to security threats and breaches."[660] In addition, EPA established a permanent Homeland Security Research Center in Cincinnati, Ohio.[661] This research center includes a Water Infrastructure Protection Division that is dedicated to overseeing ". . .research aimed at preventing deliberate contamination of the water supply, detecting and characterizing contaminants, and responding to and cleaning up contamination."[662] Furthermore, the National Drinking Water Advisory Council, an advisory body to EPA on SDWA issues, chartered a Water Secur-

657. *See id.*; *see also In Brief: $943 Million Available for Drinking Water Projects*, 36 BNA ENV'T REP. 769 (Apr. 15, 2005) (describing grant money available for drinking water projects in FY 2006).

658. *See Utilities Need More Security Information To Guard Against Terrorism*, *supra* note 331, at 331; *see also* Spence and Stoveland, *supra* note 611, at 6 ("[A]fter the initial assessment grant program, the water industry has 'dropped off the Department of Homeland Security's radar for funding needs.'").

659. WATER SECURITY WORKING GROUP FINDINGS, *supra* note 30, at v ("Security will not improve without investment of time, attention, and money on the part of all partners.").

660. *See* http://cfpub.epa.gov/safewater/watersecurity/about.cfm; *see also EPA Creates New Water Security Division To Help Defend Facilities Against Terrorism*, 34 BNA ENV'T REP. 2030-31 (Sept. 12, 2003).

661. *See EPA Creates New Water Security Division*, *supra* note 660; *see also* Andrew M. Ballard, *EPA Homeland Security Research Center To Be Made Permanent Site in Cincinnati*, 35 BNA ENV'T REP. 2405 (Nov. 19, 2004).

662. Ballard, *supra* note 661, at 2405.

ity Working Group.[663] This working group is charged with developing ". . .findings on security practices and programs, incentives for broad adoption of security practices in the water sector, and measures to gauge the implementation of security practices."[664]

Various other agencies support EPA's mission, including the Departments of Defense and Homeland Security, the Center for Disease Control, the FBI, and various other intelligence agencies.[665] For example, the Department of Homeland Security now includes an Office of Information Analysis and Infrastructure Protection that coordinates with EPA on drinking water infrastructure security issues. In addition, President Bush issued several HSPDs establishing national policies that "are of. . .particular relevance to water security issues."[666] These include HSPD-7, which established a national policy for the federal government ". . .to identify and prioritize United States critical infrastructure. . .,"[667] HSPD-8 which strengthens the country's preparedness ". . .to prevent and respond to threatened or actual domestic terrorist attacks. . .,"[668] and HSPD-9 which enhances the nation's detection and response capabilities for NBC attacks.[669] Not all of these changes are in response to the SDWA Amendments. Nevertheless, reorganizing federal and state governments to focus on drinking water infrastructure security creates the organizational structure necessary to execute this critical mission.

CONCLUSION

Drinking water in the United States has long been recognized as among the safest in the world.[670] However, "[w]e are not invulnerable to terrorism, and the consequences of a successful at-

663. *See* WATER SECURITY WORKING GROUP FINDINGS, *supra* note 30, at i.

664. *Id.*

665. *See id.*; *see also Controlling Bioterror*, *supra* note 19, at 65 (comments of Benjamin Grumbles regarding the working relationship between EPA and the CIA, FBI, and DHS).

666. *See* http://cfpub.epa.gov/safewater/watersecurity/legislation.cfm.

667. *See* Press Release, *supra* note 207, at ¶ 1.

668. *See* Press Release, *supra* note 607, at ¶ 1.

669. *See* Press Release, Office of the Press Secretary, White House, Homeland Security Presidential Directive/HSPD-9: Subject: Defense of United States Agriculture and Food at ¶ 1 (Jan. 30, 2004) *available at* http://www.whitehouse.gov/news/releases/2004/02/20040203-2.html.

670. *See* Press Release, *supra* note 5, at 1 (quoting comments of AWWA Executive Director, Jack Hoffbuhr).

tack through the water could be catastrophic."[671] Realistic threats to drinking water infrastructure components exist. Indeed, an important lesson of September 11th is that terrorists are relentless and resourceful enemies who seek to exploit previously inconceivable vulnerabilities.

The SDWA Amendments are one of the most significant results to come from the unprecedented collaboration to improve homeland security since September 11th.[672] The SDWA Amendments provide a useful framework for requiring drinking water systems to assess their vulnerabilities and increase their preparedness against intentional threats designed to disrupt their ability to provide a safe and reliable supply of drinking water. Since "[p]reparedness itself can help deter attacks," drinking water facilities complying with these requirements will be safer.[673] Because of the SDWA Amendments, awareness of drinking water infrastructure security issues has never been greater, and efforts to protect drinking water supplies have never been as focused. The SDWA Amendments have created a fundamental cultural shift in how drinking water facilities approach security, and this appears to be a lasting change.

However, much work remains to be done by both the regulated community and EPA. EPA must provide drinking water facilities with proper baseline information regarding the type of "post-9/11" threats the SDWA Amendments are intended to address. The SDWA Amendments should then be amended in several ways to require drinking water facilities to incorporate this information into their security programs. Vulnerability assessments and ERPs should be updated regularly so that they remain relevant to the current threat environment and changing facility operations. Drinking water facilities should be required to address identified infrastructure vulnerabilities by implementing best security practices. Finally, the regulatory coverage of the SDWA Amendments needs to be broadened to reach drinking water systems that serve significant populations, yet currently are not subject to the SDWA Amendments' requirements.

America's water utilities will never be immune from attack.[674] However, with specific amendments, the SDWA Amendments

671. PROTECTING OUR WATER, *supra* note 12, at 11.

672. *See id.* at 4.

673. *See* WATER SECURITY WORKING GROUP FINDINGS, *supra* note 30, at vii.

674. *See* Letter from Chairman Paul E. Gillmor to John B. Stephenson *reprinted in Controlling Bioterror: Assessing Our Nation's Drinking Water Security Hearing*

will help ensure that our nation's drinking water maintains its status as among the safest in the world.[675]

Before the Subcomm. on Env't and Hazardous Materials of the House Comm. on Energy and Commerce, 108th Cong. 78 (2004) ("It is hard to imagine a scenario in which all drinking water systems could be 'fully and completely protected'").

675. *See* PROTECTING OUR WATER, *supra* note 12, at 17.