

**U.S. Water Utilities: Terrorism Vulnerabilities,
Legal Liabilities and Protections Under the Safety Act**

**Richard J. Conway
Joseph R. Berger
Dickstein Shapiro Morin & Oshinsky LLP
January 19, 2005**

Executive Summary

The Safety Act, part of the 2002 Homeland Security Act, is designed to promote the effective use of technologies that can be deployed by governments at the federal, state and local level, and by private entities, to guard against terror attacks on vulnerable infrastructure targets.¹ One such vulnerability, where technology can be deployed to make the nation safer, is the nation's water distribution system. By the close of 2004, however, the Department of Homeland Security had only designated four technologies for protection under the Safety Act, and a burdensome application process has discouraged many applicants. Slow implementation of the Safety Act is diminishing its effectiveness and frustrating its purpose. The Act is intended to facilitate transactions by protecting not only manufacturers, but also their customers, such as the water utilities that are increasingly concerned about how to best protect their assets from a terror attack. Improved implementation by DHS will translate into:

- * faster technology deployment by water utilities to protect their distribution networks;
- * legal protections to the water utilities for those actions; and
- * expedited action in securing associated legal protection in other areas where improved technology is needed, such as security for airlines and airports, seaports and nuclear facilities.

I. The Vulnerability of U.S. Water Utility Distribution Networks

A. In the Event of a Terror Attack

These could be the headlines on the day after a terrorist attack on the water distribution network of a major U.S. city: "Thousands dead, thousands hospitalized after poisoning of city water system by terrorists using chemical pesticide; Unknown numbers may remain in need of help." So far, the headlines are only these: "Terrorists could target U.S. food and water supplies, FBI cautions; Al-Qaida is resolved to attack Americans at home, agency warns."²

Such an attack on a water distribution system could take place on a city or town, a military base, a government building, or an embassy abroad. Military bases are just as vulnerable as civilian facilities because bases generally rely upon municipal

¹ The Safety Act is codified at 6 U.S.C. §§ 441-444, further implemented at 6 C.F.R. §§ 25.1-25.9, and administered by the Department of Homeland Security. For the most current information about implementation, see www.safetyact.gov.

² Curt Anderson (Associated Press), St. Louis Post-Dispatch, September 5, 2003.

water systems.³ To target a general population, all that is necessary is an open tap in a sink or bath and a “backflow,” which can be generated inside an apartment or hotel room with a pump or vacuum and items available at a hardware store.⁴ To target a specific facility, all that is necessary is to inject poisons into the facility’s drinking water intake pipes. Poisons readily available in the domestic marketplace are capable of killing thousands if used in such a “backflow attack.” According to water industry scientists, an attack killing five to ten thousand people within 48 hours could be conducted by terrorists with commercially available products and chemicals, obtained with less than \$10,000. In the event of a backflow attack on the water distribution system of a community or facility anywhere in the world, the loss, harm and consequences could be as great as those of September 11, 2001.

B. Clear and Present Danger

This was the news following the capture of documents revealing terror plots against U.S. water systems:

The nation’s waterworks are bracing for terror attacks that could leave millions high and dry, it was revealed yesterday. Documents captured from terror master Osama bin Laden’s al Qaeda lieutenants in Afghanistan reveal that water-treatment plants are high on the list of terror targets, Time Magazine reports. The sinister plans hint that al Qaeda operatives have been investigating ways to contaminate – or disrupt – the nation’s water supply on a massive scale. The threat is so serious that the FBI issued a warning to the utilities last week. [T]he American Water Works Association – whose members supply water to 80 percent of the population – said manuals on how water treatment centers and utilities operate were recovered from al Qaeda’s lairs.⁵

Before this, in February 2002, Italian police arrested four suspected terrorists in possession of large quantities of cyanide, and with maps of the Rome water

³ Donald C. Hickman, U.S. Air Force Major, “A Chemical and Biological Warfare Threat: USAF Water Systems at Risk,” U.S.A.F. Counterproliferation Center, September 1999. Military bases are vulnerable both at home and abroad. “Pentagon officials . . . said they had on going fears about the potential for terrorists to attack the food and water supplies at American bases. They said they had been taking precautions to protect American troops being deployed in the Persian Gulf region and elsewhere overseas.” James Risen, “Threats and Responses: Terror Network; Plot to poison food of British troops is suspected,” New York Times, January 24, 2003.

⁴ See Yochi J. Dreazen, “Water Utility Officials Fear ‘Backflow’ From Terrorists; Reservoirs May Be Safe, but House Pipes Can Be Used to Push Toxins Into a Neighborhood,” The Wall Street Journal, December 27, 2001. “Water utility officials say the backflow threat dominates their post-Sept. 11 discussions with law-enforcement personnel. . . . A backflow attack . . . could spread highly concentrated amounts of poison to a few thousand homes or businesses. . . . Utility officials say that it is difficult to fully prevent a backflow incident, but they are hopeful that they can limit the damage through early detection.”

⁵ Brad Hunter, “Water Supply on High Terror Alert,” New York Post, July 15, 2002.

distribution system, marking the location of the U.S. Embassy.⁶ In May 2002, authorities signaled the alarm after a truck carrying 8 tons of cyanide was hijacked in Mexico.⁷ In May 2003, a representative for al-Qaida told a London-based Arabic-language newspaper that al-Qaida was planning to use poisons to attack the water supply of the United States.⁸ In December 2004, a Congressman on the Select Committee on Homeland Security was asking the Department of Homeland Security to ban a certain pesticide manufactured in the United States, a poison used against rabbits, coyotes, possums and other mammals.⁹ It is odorless, tasteless, the most toxic pesticide registered by the World Health Organization, the FBI believes it could be used by terrorists, and the United States has manufactured five tons annually.

Municipalities around the country are justly concerned about the possibility of an attack on their water distribution systems.¹⁰ So are municipalities in countries around the world.¹¹ There are more than 50,000 community water systems in the United States, and more than 350 of them serve populations greater than 100,000. Each drinking water utility which serves more than 3,300 people has completed vulnerability assessments and emergency response plans funded by more than \$70 million in grants from the U.S. EPA, as required by the 2002 Bioterrorism Bill.¹² The Bioterrorism Bill also

⁶ Richard Boudreaux, "[Four] Terror Suspects Arrested in Italy. . .," Los Angeles Times, February 21, 2002; Craig Whitlock, "Terror Suspects Beating Charges Filed in Europe," Washington Post, May 31, 2004.

⁷ Mary Jordan, "Mexicans search for lost cyanide; hijacking of truck carrying 7.6 tons of poison raises terrorism concerns," Washington Post, May 28, 2002.

⁸ Shaun Waterman, "Al-Qaida threat to U.S. water supply," UPI, May 28, 2003.

⁹ "Possum poison 'could be used in terror attack'; American politician calls for end to production due to US water supply threat," New Zealand Herald, December 14, 2004.

¹⁰ "Officials throughout Texas and the nation have been urged to stay on heightened alert for terrorists seeking to contaminate public drinking water supplies. . . . Information recently brought to the attention of DHS and FBI indicates that prior to the September 11, 2001 attacks, terrorists discussed possible attacks against U.S. facilities and systems to disrupt drinking water supplies serving major urban areas." Jack Douglas Jr., "Water supplies seen as potential terror targets," Fort-Worth Star-Telegram, August 17, 2004. "Terrorists linked to the al-Qaida network have tried to obtain plans for the piping systems that supply drinking water to communities across the country." Dennis Tatz, "Terrorists target water supplies; New England officials discuss safety measures," Patriot Ledger, September 25, 2002. "Many cities, with their thousands of miles of pipe, were never designed to prevent terrorists from patching into neighborhood lines and poisoning the water after it has been treated and tested for safety," Greg Winter and William Broad, "A Nation Challenged: The Water Supply," New York Times, September 26, 2001.

¹¹ "Germany: prison for threat to town's water," New York Times, May 12, 2004; "Israel TV says water supplies vulnerable to terrorist attacks," BBC, December 1, 2003; "China carries out drill to deal with water supply terror attack," BBC, September 26, 2003; "Scotland's water supplies face major risk of terrorist strike," Sunday Mail, August 24, 2003; "Danish water supplies secured against terrorism," BBC, August 14, 2003; "New Zealand police warn public of terror threats to water supply. . ." Agence France-Presse, March 10, 2003.

¹² The Public Health Security and Bioterrorism Preparedness and Response Act, or "Bioterrorism Bill," Pub. L. No. 107-188, 116 Stat. 594 (2002).

requires EPA to facilitate research on anti-terror technologies.¹³ Hundreds of water utility executives convened for a “water security congress” organized by the American Water Works Association in March 2003.¹⁴ Another is planned in 2005. In October 2003, the Government Accountability Office (GAO) released a report to Congress on how future funds to protect drinking water systems should be spent.¹⁵ In April 2004, the President signed a classified executive order designed to further promote safeguards against attacks on the water distribution networks.¹⁶ Interim voluntary security guidelines for water utilities, funded by EPA, were released in December 2004 by several industry and professional groups, addressing risks relating to management, operations, construction and design.¹⁷ Congress and the EPA have devoted considerable resources to assisting municipalities in improving security for their water distribution systems.¹⁸

¹³ Section 1434 of the Act is titled “Contaminant Prevention, Detection and Response” and section 1435, “Supply Disruption Prevention, Detection and Response.” “The Act . . . places a premium on ensuring that research is carried out to support security efforts. Section 1434 of the Act stipulates that EPA shall work collaboratively to review methods to prevent, detect, and respond to the intentional contamination of water systems, including a review of equipment, early warning notification systems, awareness programs, distribution systems, treatment technologies and biomedical research.” Statement of Benjamin H. Grumbles, U.S. EPA Acting Assistant Administrator for Water, before the Subcommittee on Environment and Hazardous Materials, Energy and Commerce Committee, U.S. House of Representatives, September 30, 2004.

¹⁴ “Protecting America’s Water Supply from Terrorists: Water Execs, Security Experts to Meet in Los Angeles,” U.S. Newswire, March 20, 2003.

¹⁵ GAO Report to the Committee on Environment and Public Works, U.S. Senate, “Drinking Water: Experts’ Views on How Future Federal Funding Can Best Be Spent to Improve Security,” October 2003. After spending \$100 million to assess vulnerabilities, Congress and EPA sought to implement security upgrades. Among the key areas recommended by GAO for funding were “physical and technological upgrades to improve security and research to develop technologies to prevent, detect, or respond to an attack (experts most strongly supported developing near real-time monitoring technologies to quickly detect contaminants in treated drinking water on its way to consumers.” *Id.* (introductory highlights).

¹⁶ Deb Riechmann (Associated Press), “President signs order to protect against bioterrorism attack; keeping water supply safe is one of features,” South Florida Sun-Sentinel, April 29, 2004.

¹⁷ “Infrastructure Security Guidelines Issued to Water Utilities; Guidelines Will Help Protect Water Supply Against Terrorist Attacks,” U.S. Newswire, December 9, 2004. The guidelines were developed by the American Water Works Association, the Water Environment Federation, and the American Society of Civil Engineers.

¹⁸ See EPA’s water security homepage, <http://epa.gov/watersecurity>. The Bioterrorism Act and several Homeland Security Presidential Directives (HSPDs), consistent with the Safe Water Drinking Act and Clean Water Act, establish EPA responsibilities for: water utility vulnerability assessments; strategies for emergency response; promotion of information exchange; and development of technological advances in water security. EPA’s “Water Security Research and Technical Support Action Plan” was released in March 2004 to respond to the mandate in the Bioterrorism Bill for research into technologies needed to address water infrastructure vulnerabilities. EPA also funds the Water Information Sharing and Analysis Center to provide drinking water and wastewater systems with early warning of potential security threats.

Water – every drop of it – is a precious natural resource that Americans once enjoyed with little thought to potential tampering by terrorists or others. Today, however . . . [t]errorist threats are targeted . . . at the country’s vital institutions and infrastructure, including drinking water and wastewater systems. To combat such threats, it is essential that government agencies, water utilities, state and local water agencies, public health organizations, emergency and follow-up responders, academia, and the private sector from across the country be ready to protect our water infrastructure. These entities are working together to reduce vulnerabilities to terrorism, prevent and prepare for terrorist attacks, minimize public health effects and infrastructure damage, and enhance recovery from any attacks that may occur.¹⁹

II. Legal Liability Resulting from a Terror Attack

A. Lawsuits and Compensation after September 11, 2001

In the days after the disaster of September 11, Congress passed a law “to preserve the continued viability of the United States air transportation system” and to compensate the victims of the attacks.²⁰ Congress created an exclusive federal cause of action for damages related to the hijackings and crashes, and lawsuits for wrongful death, personal injury, property damage and business loss were consolidated in the Southern District of New York.²¹ The law limited the airlines’ liability to the limits of the liability insurance they had maintained.²² The Safety Act adopts a similar federal cause of action and liability limit. The law of September 2001 also created the Victim

¹⁹ “EPA’s Role in Water Security Research,” U.S. EPA, August 2004, at 1.

²⁰ The Air Transportation Safety and System Stabilization Act (ATSSSA), Pub. L. 107-42, 115 Stat. 230, 230 (Sept. 22, 2001), caption.

²¹ ATSSSA § 408(b)(1). See nysd.uscourts.gov/Sept11Litigation.htm. In addition to victims’ families, owners and insurers of property in the World Trade Center and surrounding area filed a separate complaint. “WTC property damage plaintiffs file master complaint,” *Andrews Aviation Litigation Reporter*, January 21, 2003. A suit seeking \$5 billion was also filed against both manufacturer Motorola and the City of New York over hand-held radios used by firefighters, alleging product design defect, failure to warn and fraudulent misrepresentation. More than a year later, this suit was dismissed because the plaintiffs also participated in the Victim Compensation Fund. “9/11 Firefighters’ Families Sue Motorola, But Court Finds They Waived Right to Sue,” *32 Product Safety & Liability Reporter* 14, April 5, 2004. In another consolidated suit, more than a thousand workers involved in the rescue and clean-up efforts following September 11 sued the City of New York over the adequacy of safety equipment. Julius A. Rousseau III et al., “Scope of Southern District of New York’s Jurisdiction for Claims Arising From September 11, 2001,” *Mealey’s Litigation Report: Insurance*, April 13, 2004. A similar lawsuit by recovery workers over safety equipment was later filed against the leaseholder of the World Trade Center and the companies that supervised the cleanup. “Ground Zero workers file billion-dollar suit against WTC owners,” *Andrews Toxic Torts Litigation Reporter*, November 23, 2004.

²² ATSSSA § 408(a)(1). See James P Kreindler and Brian J. Alexander (lawyers for plaintiffs in September 11 suits), “September 11 Aftermath: A Perspective on the VCF and Litigation,” *18-WTR Air & Space Law*. 1, 18 (Winter 2004).

Compensation Fund, an uncapped fund that was expected to provide more than \$1 million in awards to the families of each person killed.²³ Those who elected to participate in the Fund were required to waive their right to bring lawsuits against the airlines and other defendants.²⁴

Many lawsuits were filed nonetheless, pleading joint and several liability against many defendants. In the suits relating to the World Trade Center, defendants include the manufacturer of the two hijacked aircrafts; the three airlines which carried the terrorists; and the many other airlines participating in the joint security system at the Portland airport in Maine and Logan airport in Boston, through which the terrorists passed. Defendants also include the many security contractors at the airports, and the City of Portland and the Massachusetts Port Authority, which operated the airports.²⁵ Defendants also include the Port Authority of New York and New Jersey, owner of the Trade Center; the corporate lessees of the Trade Center; and the corporations that designed the Trade Center. At one point, more than a thousand suits by families were filed against the Port Authority, which itself lost employees on September 11.²⁶ Among the counts alleged in these suits are claims based on negligence, reckless conduct, conscious disregard for rights and safety, *res ipsa loquitur*,²⁷ negligent infliction of emotional distress, punitive damages, and negligent selection of security contractors. Against the manufacturer, the claims also include strict tort liability, negligent design and breach of warranty. The defendants to these lawsuits filed motions to dismiss, and most of these motions were denied in September 2003, in a decision that allowed the lawsuits to proceed.²⁸

As of 2004, about a hundred families chose to pursue lawsuits instead of the Victim Compensation Fund.²⁹ It was reported that “the flood of litigation is occurring

²³ Diana B. Henriques and David Barstow, “A Nation Challenged: Victims’ Compensation; Fund for Victims’ Families Already Proves Sore Point,” *New York Times*, October 1, 2001.

²⁴ Two years later, the average award for loss of life was \$1.6 million, and less than half of victim’s families had applied to the Fund. Diana B. Henriques, “Concern Growing as Families Bypass 9/11 Victims’ Fund,” *New York Times*, August 31, 2003. Meanwhile, many lawsuits against the airlines were filed as statute of limitation deadlines approached. Benjamin Weiser, “Two Years Later: Lawsuits; Families of Victims File to Meet a Legal Deadline,” *New York Times*, September 11, 2003. Many plaintiffs ultimately abandoned their lawsuits with the approach of the deadline for participation in the Victim Compensation Fund on December 22, 2003. David W. Chen, “Applicants Rush to Meet Deadline for Sept. 11 Fund,” *New York Times*, December 23, 2003.

²⁵ Plaintiffs’ Amended Flight 11 Master Liability Complaint; Plaintiffs’ Amended Flight 175 Master Liability Complaint, *In Re September 11, 2001 Litigation*, No. 21 MC 97 (AKH) (S.D.N.Y.).

²⁶ “Sept. 11 Anniversary Marks Lawsuit Deadline for Port Authority,” *BestWire*, Sept. 12, 2002; David W. Chen, “Suits by 950 Families Allege Safety Lapses at the Towers,” *New York Times*, September 14, 2002.

²⁷ *Res ipsa loquitur* is the common law doctrine regarding injuries that normally do not occur in the absence of negligence, which may be inferred from the injuries themselves.

²⁸ *In re September 11 Litigation*, 280 F.Supp.2d 279 (S.D.N.Y. 2003). See Diana B. Henriques and Susan Saulny, “Two Years Later: Lawsuits; Judge’s Ruling Opens Door for More Families to Sue Airlines and Port Authority,” *New York Times*, September 10, 2003.

²⁹ Kreinder and Alexander, *supra* note 22, at 19.

despite the work of the . . . Fund, which Congress established, not only to help those directly harmed by the Sept. 11 plane crashes, but also to protect the airlines from lawsuits.”³⁰ By the time the Fund finished its work, it had paid about \$7 billion in awards to families of those killed or injured.³¹ Compensation from all sources to all victims of the attacks, including families of those killed, people injured and businesses with property loss, has totaled \$38.1 billion to date, of which \$23.3 billion went to businesses.³² Insurance companies account for \$19.6 billion of the total; government entities, about \$16 billion; and private charities the remainder.

B. Municipal Utility Liability Resulting from a Backflow Attack

In the legal aftermath of a backflow attack, as explained below, the entities to be sued would likely include the municipal or private water utility or utilities providing services where the attack occurred, and the manufacturers and operators of any technology employed to protect the water system.³³ In addition to the hundreds of municipal water utilities around the country, there are many large private utilities, some publicly traded, that serve the public and municipal customers, including 45 million people in the United States and Canada.

The majority of the U.S. population is served by community water systems that are publicly owned and operated. States generally benefit from sovereign immunity in state and federal courts, but the Supreme Court has noted that sovereign immunity “does not extend to suits prosecuted against a municipal corporation or other governmental entity which is not an arm of the State.”³⁴ Most states have waived sovereign immunity in their own courts to varying degrees by “Tort Claims Act” statutes, such as those by that name in New Jersey, Florida, Texas, California, Maryland and Virginia, and the New York Court of Claims statute. These statutes are in turn subject to interpretation by the respective state common law, which often classifies state actions into categories of governmental and/or discretionary functions which are immune, and proprietary³⁵ and/or non-discretionary functions which are not.³⁶ As a general matter, municipal utilities benefit little from sovereign immunity:

³⁰ Leslie Eaton, “Lingering 9/11 anger finds its outlet in courts,” *International Herald Tribune*, September 10, 2004.

³¹ David W. Chen, “Striking Details in Final Report on 9/11 Fund,” *New York Times*, November 18, 2004.

³² David W. Chen, “New Study Puts Sept. 11 Payout at \$38 Billion,” *New York Times*, November 9, 2004 (discussing the study by Rand Corp.).

³³ “For example, a manufacturer of a chemical or biological agent detection device could face one or several class action suits worth billions of dollars if the equipment they produced failed to prevent an attack using one of these agents. This prospect has made government contractors . . . cautious about the programmes in which they choose to participate.” Mary Dinh and Seth Drewry, “The SAFETY Act’s impact on US homeland security,” *Janes.com*, July 20, 2004.

³⁴ Alden v. Maine, 527 U.S. 706, 756 (1999).

³⁵ Meaning an activity conducted for the benefit of the municipality as a corporate entity rather than for the benefit of the public. “When a municipality is in the business of selling water to customers for profit or revenue, it is engaged in a proprietary function.” Junior College District of St. Louis v. City of St. Louis, No. SC 85583, 2004 WL 2663621 (Mo. Nov. 23, 2004) (en banc). Even a state can sue a municipality

Because many public water suppliers are quasi-governmental, the defense to claims of liability has often been that, as public water suppliers, they are performing a governmental function and, thus, are insulated from liability. The courts have routinely rejected this view, holding that, with the exception of emergencies, public water suppliers are operating in a 'proprietary' rather than governmental capacity.³⁷

Municipal water utilities and operators would also have little protection in the event their water supplies are deliberately compromised. Commentators agree that municipal utilities could become liable following a terror attack. According to members of the American Bar Association Water Resources Committee, just as lawsuits followed the attacks on the World Trade Center in both 2001 and 1993,

[S]imilar lawsuits can be expected when water supplies or infrastructure are sabotaged. For many water utilities, a large award could undermine their financial ability to continue providing needed services. Even a claim could affect a utility's bond rating.

Utilities would be sued under negligence theories. . . . Ironically, legal actions may arise from attempts to make public water supplies more secure. For example, EPA's recently issued guidelines detail the security measures water utilities are advised to implement immediately. If a particular utility fails to implement some or all of these measures or does so in a negligent manner, then the utility arguably should be liable for consequential damages. In the numerous jurisdictions where comparative

over negligence in the maintenance of municipal water lines. State of Texas v. City of Galveston, No. 01-03-00557-CV, 2004 WL 2066448 (Tex. App. Sept. 10, 2004).

³⁶ New York maintains the "general rule that a municipality may be liable if its agents are acting in a proprietary capacity, but not, absent some special undertaking, in a governmental capacity." Stewart F. Hancock, Jr., "Municipal Liability Through a Judge's Eyes," 44 Syracuse L. Rev. 925, 936 (1993). In Florida, "several decades of Florida Supreme Court decisions construing Florida's waiver statute have generated a body of case law [such that] there are no defined legal boundaries of governmental tort liability and there is no clear framework with which to analyze immunity." Thomas A. Bustin and William N. Drake, Jr., "Judicial Tort Reform: Transforming Florida's Waiver of Sovereign Immunity Statute," 32 Stetson L. Rev. 469, 469-470 (2003). In Texas, a municipality is by statute liable "for damages arising from its governmental functions . . . including . . . health and sanitation services." Tara L. Shaw, "Is Texas Waiving Good-bye to Sovereign Immunity?," 3 Tex. Tech. J. Tex. Admin. L. 225, 232 (2002).

³⁷ Sarah J. Meyland, "Land Use & The Protection of Drinking Water Supplies," 10 Pace Env'tl. L. Rev. 563, 587 (1993). In the context of ordinary utility activities, "there is agreement . . . that the doctrine of sovereign immunity affords no protection to a municipal water distributor guilty of negligence in regard to the escape of water from its service pipes," and "[i]t has been held that a water distributor may incur liability for negligently maintaining service pipes in such a condition that impure water is furnished to the consumer." "Water Distributor's Liability for Injury Due to Condition of Service Lines, Meters, and the Like, Which Service Individual Consumer," 20 A.L.R.3d 1363, § 2 (2004).

negligence applies, a utility theoretically could be held liable for some portion of the damages upon a showing of minimal negligence.³⁸

And according to the Interim Voluntary Security Guidance for Water Utilities released in December 2004,

Court rulings have found that a water utility must exercise reasonable care in operating and maintaining its system. The definition of ‘reasonable care’ is key in determining liability. As more water utilities implement security improvements, it could be argued that the definition of reasonable care is evolving to include installation of security systems that only a short time ago were rarely found in water systems.³⁹

C. Liability of Technology Providers

Water utilities require equipment and technology provided by the private sector to improve security measures against a backflow or other terror attack. These companies will also be vulnerable to lawsuits, even if their technology works as intended. Despite the massive resources devoted to the problem, no technology can stop all harm in all possible situations. In the event of an attack, lives can be saved with reliable technology deployed in an appropriate manner, but manufacturers expect lawsuits against them in the case of such an event, regardless of how their technology performs. This expectation affects the choices companies make about whether it is worthwhile to pursue anti-terror technologies at all. In fact, one of the first companies to receive protection under the Safety Act has thus far declined to bring its product to market, because the insurance it is required to maintain is too expensive.⁴⁰ Most companies seeking protection have yet to receive it under the Act:

³⁸ Tim De Young and Adam Gravley (chairs of the ABA Water Resources Committee), “Coordinating Efforts to Secure American Public Water Supplies,” 16-WTR Nat. Resources & Env’t 146, 152 (2002). “Some water utility officials believe that the leading threat to the nation’s water supply may be the use of backflow pressure to introduce poisons into local water distribution systems.” *Id.* at 147.

³⁹ American Society of Civil Engineers, American Water Works Association, and the Water Environment Federation, “Interim Voluntary Security Guidance for Water Utilities” at 1.2.2.2., December 9, 2004 (“Legal and Liability Issues”). “Once a vulnerability assessment is complete, the resulting recommendations . . . could be considered as notice of a dangerous condition. This notice could potentially result in liability if the recommendations are not addressed.” *Id.*

⁴⁰ Tim Starks, “Best Laid Plans: Effort to Lure Homeland Business With Liability Protection Falls Far Short of Goals,” Congressional Quarterly Homeland Security, January 7, 2005. “And for companies that have not won the protections of the Safety Act yet, industry officials said, the best work to describe their view of the law so far is frustrated. Many that have applied have found the process maddening, and some companies have not even bothered to apply because of the expectation that it is not worth the trouble.” Insurance costs for another company to win Safety Act designation, a small security firm, have ballooned from \$5,000 per year prior to September 11, 2001 to more than \$500,000. Robert Block and J. Lynn Lunsford, “U.S. Gives Liability Protection to Antiterror Firms,” The Wall Street Journal, June 18, 2004.

More than one year after the Department of Homeland Security issued an interim regulation on granting liability protections to anti-terror technology manufacturers, six months after the first batch of companies to receive the protections were announced, and four approvals out of more than 200 applications later, the law meant to encourage businesses to get into the homeland security market has apparently had little effect.⁴¹

D. Liability Protection Under the Safety Act

In the event of the hypothetical terror attacks described above, a water utility could be sued for failure to take appropriate or recommended actions to protect its water distribution network. But even if it does take all feasible actions to prevent such an attack, it faces lawsuits over any technologies used to protect its network.

Consider a scenario in a major city where a contaminant detection device alerts utility workers to a safety hazard involving a portion of the distribution network serving apartment buildings, in the evening hours after most of the city has gone home.⁴² The utility workers quickly take all necessary actions, as they have practiced to do under government mandates for emergency preparedness. They alert appropriate utility personnel and government officials while investigating the hazard. They confirm the extent of the danger and relay the news to government officials, who initiate a civil emergency notification to the public over the broadcast networks. For the next several hours, newscasters urge the public not to touch their water at home, families and friends alert each other on cell phones, and utility officials launch steps necessary to protect the public. Utility workers determine that the source of contamination appears to result from a deliberate attack, and the FBI and city police prepare SWAT teams for action. Urgent communications allow for precautions in other cities. The utility narrows down the possible locations of a backflow, and with the help of an alert public, the perpetrators are caught. Lives are saved and by morning, it is announced to the public what steps need be taken to safely resume water use, while further remediation is conducted. But it is reported that many have been injured, and some lives have been lost. Congress convenes and announces aid to the victims and their families.

If the technology employed by the utility is not “designated” under the Safety Act, as explained below, the utility can be sued over its use and operation of the device, whether it fails or functions perfectly. If the technology employed is designated under

⁴¹ Starks, *supra* note 40.

⁴² EPA has assisted utilities in preparation of emergency response plans for similar scenarios by issuing the December 2003 “Response Protocol Toolbox: Planning for and Responding to Drinking Water Contamination Threats and Incidents.” “Utility staff possess an extensive knowledge about the physical configuration, operation, and water quality of their system. This knowledge should be utilized throughout the entire threat evaluation process. . . . Furthermore, during advanced stages of an incident, the understanding of distribution system hydraulics by operations staff and engineers will be critical to the rapid assessment of the propagation of a suspected contaminant through a system.” Module 2: “Contamination Threat Management Guide,” at 27.

the Act, any suit relating to the performance of the device cannot be brought against the utility. And in the event that some form of suit is allowed against the utility relating to the device, the insurance maintained by the manufacturer is required to cover any liabilities of the utility. If the device functions as designed, the manufacturer also receives protection under the Act. In the event the device is defective and fails due to negligence of a manufacturer, the courts would have the power to allow a remedy, which would be against the manufacturer alone, and covered by its insurance. Consider an alternative scenario where the detection device was never deployed in the first place, allowing for a hundredfold increase in the level of harm and injury.

III. The Safety Act

A. The Safety Act Statute

Congress enacted the Safety Act in order to promote the use of effective technology to combat terrorist threats, and to offer manufacturers of such technology necessary protection from product liability lawsuits.⁴³ “The Select Committee [on Homeland Security] believes that technological innovation is the Nation’s front-line defense against the terrorist threat.”⁴⁴ Part of the Homeland Security Act of 2002, the Safety Act is formally titled the Support Anti-Terrorism By Fostering Effective Technologies Act of 2002.⁴⁵ The Safety Act authorizes the Homeland Security Secretary to designate “qualified anti-terrorism technologies” to receive certain protections (referred to as QATT or qualified ATTs, which can refer to products and/or services).⁴⁶ The DHS wrote regulations to implement the Safety Act, issuing a Proposed Rule on July 11, 2003 and an Interim Rule on October 16, 2003.⁴⁷ According to the Proposed Rule, the purpose of the Act “is to ensure that the threat of liability does not deter potential manufacturers or [s]ellers of anti-terrorism technologies from developing and commercializing technologies that could save lives.”⁴⁸ There are two levels of protection for technologies under the Act, provided first by “designation” as qualified

⁴³ See Homeland Security Act of 2002, Pub. L. No. 107-296, 16 Stat. 2135; H.R. Rep. No. 107-609(I) (2002), reprinted in 2002 U.S.C.C.A.N. 1352, 1399.

⁴⁴ H.R. Rep. No. 107-609(I), 2002 U.S.C.C.A.N. 1352, 1399. “Unfortunately, the Nation’s products liability system threatens to keep important new technologies from the market where they could protect our citizens. In order to ensure that these important technologies are available, the Select Committee believes that it is important to adopt a narrow set of liability protections for manufacturers of these important technologies.”

⁴⁵ Part G of Title 6, 6 U.S.C. §§ 441-444. Title 6 is the Domestic Security Title of the United States Code.

⁴⁶ 6 U.S.C. § 441. QATT is to be designated according to certain listed criteria which include magnitude of risk exposure to the public if technology is not deployed, and likelihood that the technology would not be deployed without protections of the Safety Act. § 441(b). QATT is defined to include “any product, equipment, service . . . device, or technology . . . designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause, that is designated as such by the Secretary.” § 444(1).

⁴⁷ Regulations Implementing the [Safety Act], 68 Fed. Reg. 41,420 (proposed July 11, 2003) (“Proposed Rule”); 68 Fed. Reg. 59,648 (Oct. 16, 2003) (“Interim Rule”) (codified at 6 C.F.R. pt. 25).

⁴⁸ Proposed Rule, 68 Fed. Reg. at 41420.

ATT, and second at a higher level by “certification” as an Approved Product. Applications for both designation and certification are available on the DHS Safety Act website.⁴⁹

1. Benefits for Designated Anti-Terror Technologies

The Act establishes a “litigation management” framework, and an exclusively federal cause of action, for “claims arising out of . . . an act of terrorism when qualified anti-terrorism technologies have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller.”⁵⁰ Among the protections for defendants under this framework, federal jurisdiction is exclusive, no punitive damages are allowed, non-economic damages are limited (joint liability is prohibited and physical injury is required for such), and awards are reduced by collateral sources (such as insurance).⁵¹ The federal cause of action applies to injuries related to technologies sold to both the federal government and other customers (including state and local governments and commercial entities).⁵² **The Act thus provides a limited legal recourse to parties who believe they were injured by failure of designated technologies.**

The appropriate federal district court is granted jurisdiction “over all actions for any claim for loss of property, personal injury, or death arising out of, relating to, or resulting from an act of terrorism when qualified [ATTs] have been deployed. . . .”⁵³ Furthermore, “[s]uch Federal cause of action shall be brought only for claims for injuries that are proximately caused by sellers that provide [QATT].”⁵⁴ The DHS has set forth its view that under these provisions, “only one Federal cause of action exists for loss of property, personal injury, or death when a claim relates to performance or non-performance of the Seller’s qualified and deployed anti-terrorism technology, and (2) such cause of action may be brought only against the Seller.”⁵⁵ **The Act thus protects the seller’s customers against the filing of lawsuits relating to the performance of designated technologies.**

The Act next provides a “risk management” framework that requires sellers of qualified ATTs to obtain liability insurance against third party claims in an amount certified by the Secretary, and “which will not unreasonably distort the sales price” of

⁴⁹ See www.safetyact.gov.

⁵⁰ 6 U.S.C. § 442(a)(1).

⁵¹ 6 U.S.C. § 442(b).

⁵² The substantive law is that of the state where the act of terrorism occurs, except where preempted by federal law. § 442(a)(1). The term “non-federal government customers” is defined in § 444(6).

⁵³ 6 U.S.C. § 442(a)(2).

⁵⁴ 6 U.S.C. § 442(a)(1).

⁵⁵ Preamble to the Proposed Rule, 68 Fed. Reg. 41420, 41423. This is “the best reading” of these provisions, and “the reading the Department is inclined to adopt.” *Id.* Under Supreme Court caselaw, federal courts give deference to an agency’s reasonable interpretation of a statute or its own regulations.

the technology.⁵⁶ Liability for all claims against a seller (including contribution and indemnity) “shall not be in an amount greater than the limits of liability insurance coverage required to be maintained by the Seller under this section.”⁵⁷ DHS has discretion to determine the amount of liability insurance required to be maintained.⁵⁸ The features of the Safety Act creating a federal cause of action and establishing liability limits tied to insurance coverage are similar to the analogous provisions in the law enacted in September 2001 to protect the airline industry following the disaster.⁵⁹ **The Act thus requires liability insurance and proportionate liability limits to protect the seller and provide recovery to plaintiffs.**

In addition, under the risk management framework, the required insurance:

shall, in addition to the Seller, protect the following, to the extent of their potential liability for involvement in the manufacture, qualification, sale, use or operation of [qualified ATTs]: (A) Contractors, subcontractors, suppliers, vendors and customers of the Seller. (B) Contractors, subcontractors, suppliers, and vendors of the customer. Such liability insurance under this section shall provide coverage against third party claims arising out of, relating to, or resulting from the sale or use of anti-terrorism technologies.⁶⁰

The seller is required to enter into reciprocal waivers of claims with its contractors, subcontractors, suppliers, vendors and customers, and contractors and subcontractors of the customers.⁶¹ **The Act thus further protects the seller’s customers in the event any actions are allowed related to the use and operation of technology, which are covered by the seller’s insurance and liability limit.**⁶²

⁵⁶ 6 U.S.C. § 443(a)(1),(2).

⁵⁷ 6 U.S.C. § 443(c).

⁵⁸ 6 C.F.R. § 25.4(h).

⁵⁹ With the Safety Act, “Congress balanced the need to provide recovery to plaintiffs against the need to ensure adequate deployment of anti-terrorism technologies by creating a cause of action that provides a certain level of recovery against Sellers, while at the same time protecting others in the supply chain.” Interim Rule, 68 Fed. Reg. at 59693.

⁶⁰ 6 U.S.C. § 443(a)(3),(4).

⁶¹ 6 U.S.C. § 443(b).

⁶² Under the interpretation of DHS, no lawsuits can be brought against customers for the performance or non-performance of qualified ATTs. This interpretation should also foreclose lawsuits related to the use or operation of qualified ATTs. But in the event that any kind of lawsuit is allowed by a court relating to the ATTs, the customer is still protected by the seller’s insurance and liability limits. Without Safety Act designation, a customer could seek protection through its own insurance, but it would not benefit from the liability limitation that exists under the Safety Act.

2. The Government Contractor Defense for Certified Technologies

The litigation management section of the Act also provides for an additional benefit, the Government Contractor Defense (GCD), for technologies that are certified by DHS as “Approved Products.”⁶³ There “shall be a rebuttable presumption that the [GCD] applies” where a qualified ATT is subject to a product liability or other lawsuit, the presumption overcome only with evidence that the seller acted fraudulently in submitting information to the DHS Secretary. This defense applies to a sale of the product to either the federal government or other customers (including state and local governments and commercial entities).

For certification as an Approved Product, additional steps by the applicant and DHS are needed beyond “designation” as qualified ATT. “Upon the Seller’s submission to the Secretary for approval of anti-terrorism technology, the Secretary will conduct a comprehensive review of the design of such technology and determine whether it will perform as intended, conforms to the Seller’s specifications, and is safe for use as intended.”⁶⁴ Once the Secretary approves a technology, a “certificate of conformance” is issued and the technology is placed on an “Approved Product List for Homeland Security.”⁶⁵

The Government Contractor Defense is a common law defense to tort liability established by the Supreme Court in a 1988 case, Boyle v. United Technologies Corp.⁶⁶ The common law protects manufacturers from design defect lawsuits when their designs were approved by the federal government. The primary distinction involving the GCD codified by the Safety Act is that once a product is certified, the GCD applies whether the product is sold to the federal government, a state or local government, or even a private entity. This expands the scope of protection offered to manufacturers, which is intended to encourage the development of needed technologies, and the sale of those technologies to the parties that need them most. In addition, sellers of technology need not design their technologies to government specifications in order for the GCD to apply under the Safety Act to a certified technology.⁶⁷ According to DHS, “it is clear that any Seller of an ‘approved’ technology cannot be held liable under the Act for

⁶³ 6 U.S.C. § 442(d)(1).

⁶⁴ 6 U.S.C. § 442(d)(2).

⁶⁵ 6 U.S.C. § 442(d)(3).

⁶⁶ 487 U.S. 500 (1988). The Court held that a federal government contractor could not be held liable under state product liability law for defects in military equipment when “(1) the United States approved reasonably precise specifications; (2) the equipment conformed to those specifications; and (3) the supplier warned the United States about the dangers in the use of the equipment that were known to the supplier but not to the United States.” 487 U.S. at 512. The Supreme Court concluded that “state law which holds Government contractors liable for design defects” presents a conflict with federal policy and “must be displaced.” Id.; see also Proposed Rule, 68 Fed. Reg. at 41422.

⁶⁷ See Proposed Rule, 68 Fed. Reg. at 41422.

design defects or failure to warn claims, unless the presumption of the defense is rebutted.”⁶⁸

The Safety Act leaves some questions about the statute’s use of the common law unanswered.⁶⁹ For instance, in a situation where common law defenses would also be available to the contractor, would the statute’s provision offer additional protection? Commentators have stated that the burden of proof under the statute should be more favorable to the manufacturer than under the common law, and DHS has affirmed this view.⁷⁰ The DHS has also stated its view that “Congress incorporated the Supreme Court’s Boyle line of cases as it existed on the date of enactment of the Safety Act, rather than incorporating future developments. . . .”⁷¹ The common law has developed differences among the federal circuit court jurisdictions. For instance, many circuits have held that manufacturing defects are not covered by the GCD, but their rulings differ on this point.⁷² Were the common law of manufacturing defects to be interpreted under the Safety Act, courts would need to strike a balance between the purpose of the Act, the intended protection of manufacturers, and the rights of injured victims in a case where a manufacturer was truly negligent. Thus, the Act itself strikes an appropriate balance between these interests.

3. The Safety Act is the Proper Vehicle for Government Indemnification to Contractors

On February 28, 2003, President Bush issued Executive Order 13286, granting responsibilities to the DHS Secretary, amending previous executive orders, and limiting the previously existing ability of federal agencies to provide indemnification to government contractors under Public Law 85-804 for “risks that the contract defines as unusually hazardous or nuclear in nature.”⁷³ The Defense Department is required to evaluate whether the Safety Act would be a more appropriate vehicle for indemnification, and determine that indemnification “is necessary for the timely and effective conduct of United States military or intelligence activities,” before granting

⁶⁸ Id.

⁶⁹ See Alison M. Levin, “The Safety Act of 2003: Implications for the Government Contractor Defense,” 34 Pub. Cont. L.J. 175 (2004).

⁷⁰ See Levin, *supra*, at 193-194. See also Interim Rule, 68 Fed. Reg at 59687. “[T]he Department believes that Congress intended that, for purposes of applying the GCD, courts presume that all of the legal and factual requirements for establishment of the GCD by a government contractor are met by the existence of an applicable SAFETY Act Certification.”

⁷¹ Proposed Rule, 68 Fed. Reg. at 41,422.

⁷² See Levin, *supra*, at 183-190.

⁷³ See Proposed Rule, 68 Fed. Reg. at 41425. “Congress intended that the Safety Act’s liability protections would substantially reduce the need for the United States to provide indemnification under Public Law 85-804 to [s]ellers of anti-terrorism technology.” Contractual indemnification to contractors may be provided under Public Law 85-804 and Executive Order 10789 (November 14, 1958), as amended by Executive Order 11610 (July 22, 1971), and pursuant to regulations at Part 50 of the Federal Acquisition Regulation (for “risks that the contract defines as unusually hazardous or nuclear in nature”).

indemnification through a contractual provision under P.L. 85-804.⁷⁴ Any other agency considering a contractor's request for indemnification for a product or service that could qualify under the Safety Act as QATT must first consult with DHS and the Office of Management and Budget. The DHS must advise whether Safety Act protection would be more appropriate, and if the agency wishes to provide indemnification, it must receive approval from the OMB.

This Executive Order has affirmed the Safety Act as the proper and appropriate vehicle for provision of liability protection to federal government contractors. Some major defense contractors have taken the position that they will not bid on certain contracts for anti-terrorism services or products without Safety Act protections.

B. Implementation by the Department of Homeland Security

The Interim Rule delegates Safety Act responsibilities to the DHS Under Secretary for Science and Technology.⁷⁵ By this rule DHS also created the application process for both designation and certification.⁷⁶ The certification process is largely the same as the designation process.⁷⁷ Certification may be conditioned upon any specifications that the Under Secretary finds appropriate.⁷⁸ Application kits are available on the DHS website.⁷⁹ DHS has also provided for pre-applications to be reviewed within 21 days, with feedback provided to assist businesses in how best to proceed. Within 90 days after a full application is received, the Assistant Secretary for Plans, Programs, and Budget is to make a recommendation to the Under Secretary that the application be approved or denied, or that additional information is required, and may also extend this time period.⁸⁰ The Under Secretary must likewise issue a decision, request additional information, or determine that additional time is necessary, within 30 days.⁸¹

In December 2004, the National Defense Industry Association (NDIA) held a two-day meeting to discuss implementation of the Act. At that time, 153 pre-applications had been submitted to DHS, and 50 final applications. Two had been denied and only four had been approved.⁸² DHS had stated to Congress that it believes

⁷⁴ Executive Order 13286 (February 28, 2003) at § 73.

⁷⁵ 6 C.F.R. § 25.2.

⁷⁶ 6 C.F.R. §§ 25.3, 25.5 (designation), 25.7 (certification).

⁷⁷ 6 C.F.R. § 25.7(a). A certification application cannot be filed without a designation application, and DHS may not issue a certification without a designation.

⁷⁸ 6 C.F.R. § 25.7(g).

⁷⁹ See www.safetyact.gov.

⁸⁰ 6 C.F.R. §§ 25.5(d); 27.5(d).

⁸¹ 6 C.F.R. §§ 25.5(e); 27.5(e).

⁸² "Department of Homeland Security Announces First Designations and Certifications Under the Safety Act," Office the Press Secretary, Department of Homeland Security, June 18, 2004. The technologies designated were Lockheed Martin Corp.'s Risk Assessment Platform, which is a computer operating

that, while the time needed to complete an application varies according to the size of the company involved, the average time has been about 150 hours.⁸³ According to members of the NDIA, the time required to prepare a full application has been as much as 1000 to 1600 hours.⁸⁴ In December 2004, DHS announced it had prepared a draft revision of the application kit and sought additional comments on the application process.⁸⁵

The chairs of the House Judiciary Committee, Committee on Government Reform, and the Select Committee on Homeland Security wrote to DHS Secretary Tom Ridge in May 2004, in order to relay their concerns about Safety Act implementation.⁸⁶ The chairs wrote that “As the statute itself suggests, the analysis to be undertaken by the Department for the designation and certification of a given technology was intended to be simple and straightforward – a means of *facilitating* transactions, *not* erecting additional barriers to deployment.”

The Congressmen wrote that “It is absolutely essential that the Department initiate a process to prioritize applications for Safety Act designation and certification, and ensure that critical technologies receive expedited treatment.” Further, the chairs did not view this process as “requiring the Department to insert itself in a pending transaction for the purpose of establishing performance standards for a given technology. . . .”⁸⁷ “Where pending procurements are involved, the Department should defer to the judgment of the buyer and utilize information already provided in connection with the procurement, rather than reconstruct a process the parties already have diligently undertaken.”

framework designed to conduct security risk assessment; Michael Stapleton Associates’ SmartTech System, which is designed for screening of items for explosives and hazardous materials; Northrop Grumman’s Biohazard Detection System, which analyzes mail for anthrax and other pathogens; and Teledyne Brown Engineering’s Mobile Fluid Jet Access System, which is designed to cut through explosive devices with a high-powered water stream.

⁸³ Letter from Charles E. McQueen, DHS Under Secretary for Science and Technology, to Representative Christopher Cox, June 14, 2004.

⁸⁴ See Starks, *supra* note 40.

⁸⁵ “Revision of Currently Approved Information Collection Requests for [SAFETY] Act of 2002,” 69 Fed. Reg. 72207 (Dec. 13, 2004); see also Starks, *supra* note 40.

⁸⁶ Letter from James Sensenbrenner, Jr., House Judiciary Committee Chair, Christopher Cox, Select Committee on Homeland Security Chair, and Tom Davis, House Committee on Government Reform Chair, to the Honorable Tom Ridge, DHS Secretary, May 11, 2004.

⁸⁷ The letter continued: “If, for example, a city government and an anti-terrorism technology manufacturer have negotiated a contract to purchase biohazard detectors, and have made consummation of the deal contingent upon Safety Act designation and certification of the biohazard detectors, the Department’s review should not involve a *de novo* determination of whether the detectors meet a particular performance standard. . . . Unless the design or operation of the product itself poses inherent risks to the public, the technology should be promptly designated or certified.”

The Department replied to the Congressmen in June 2004 by letter from the Under Secretary for Science and Technology, Charles E. McQueen.⁸⁸ Mr. McQueen wrote that “While I understand your concerns and your desire for a more streamlined process, I believe the process we have implemented is consistent with the minimum requirements of the Act.” Mr. McQueen responded to the specific points raised by the Congressmen, agreeing with some and disagreeing with others, such as the role of DHS when a transaction is pending between a municipal government and technology manufacturer. This issue has come to the forefront because today, municipalities are proceeding to respond to terror threats with the help of private technology partners, while these parties do not yet benefit from protections under the Safety Act, as Congress intended. In addition, procurements are proceeding that bidders seek to make contingent upon protection under the Act. Uncertainty over the status of anti-terror technologies in turn affects the willingness of parties to enter into transactions related to those technologies. These procurement issues may yet be addressed by the Department in future policies and rulemakings.

The future of the Safety Act, like the future nature of terror threats, is uncertain, but the risks of terror threats are sure to remain. The protection of water distribution systems is just one example where needed improvements cannot occur without the deployment of new technology. Municipal entities and their private partners have a duty to improve security, and face liability if they fail to take appropriate measures recommended by the industry. But providers of technology face liability simply by offering the needed protection, and many will not provide it without the application of the Safety Act. If the Safety Act functions as Congress intended, it will encourage the deployment of these technologies, designed and needed to improve national security. In order for this to occur, the Department of Homeland Security must do more to facilitate the assessment of applications for designation and certification under the Act. The provisions afforded by the Act protect not only manufacturers, but the very entities responsible for infrastructure security, be they federal agencies, states, municipalities, or their private partners. With maximum implementation by DHS, the Safety Act will facilitate their efforts to protect the public with the most robust security measures that technology can provide.

⁸⁸ Letter from Charles E. McQueen, DHS Under Secretary for Science and Technology, to Representative Christopher Cox, June 14, 2004.