Protecting the Water Sector from Security Threats

The Emerging Legal and Policy Frameworks

Table of Contents

Introduction

The United States and its public and private institutions have evolved dramatically since 2002, when the National Association of Clean Water Agencies (NACWA) published, *"Protecting Water Infrastructure Assets...Legal Issues in a Time of Crisis Checklist" (Checklist)*. The *Checklist* was published in the wake of September 11, 2001, and the attacks on the World Trade Center and the Pentagon. Since then, terrorist attacks have continued around the world, adding impetus for the prompt establishment of the Department of Homeland Security and passage of numerous federal security statutes and the promulgation of implementing regulations which touch every aspect of American life. As a result, NACWA has partnered with the American Public Works Association (APWA), the Association of Metropolitan Water Agencies (AMWA), and the Water Environment Federation (WEF) to expand, revise, and update the issues covered in the *Checklist* as a result of the unprecedented legal, technical, and policy changes in protecting the nation's critical water sector infrastructure over the last five years.

The above organizations have worked with Dewey & LeBoeuf, and its Senior Counsel, Robert M. (Andy) Andersen, who also teaches environmental security as an Adjunct Professor at George Washington University, to prepare this publication studying the legal and policy frameworks that govern key aspects of security at drinking water and wastewater treatment facilities, and public works management overall. This publication replaces the original *Checklist*.

This publication, *Protecting the Water Sector from Security Threats: The Emerging Legal and Policy Framework*, is protected by copyright owned by APWA, AMWA, NACWA, and WEF, and may not be reproduced, stored, or transmitted in any form or by any means without the consent of these organizations. This publication contains information on legal and policy issues associated with the management of security risks at publicly and privately owned water sector infrastructure, defined to included drinking water facilities and distribution systems, wastewater treatment facilities, associated collection systems, and stormwater systems. This document should not be construed as legal advice to member agencies or others who might refer to it. The availability of this publication does not replace the need to conduct an independent evaluation of relevant issues. There is no representation, expressed or implied, that this information is suitable for any particular situation. APWA, AMWA, NACWA, and WEF have no obligation to update this work or make notification of any changes to the information discussed in the work. APWA, AMWA, NACWA, WEF, Dewey & LeBoeuf, the publication's principal author, Robert M. Andersen, and the individuals who reviewed or contributed to this publication's content do not assume any liability resulting from the use or reliance upon any information, guidance, suggestions, conclusions, or opinions contained herein.

The *Checklist for Owners and Operators* found the end of this publication is designed to help water and wastewater facilities in identifying the major legal issues facing the water sector in the current security environment. It is not intended to be an exhaustive list of legal issues but is instead meant to help owners, operators, and public works managers understand the most important legal considerations when working to secure critical water sector facilities.

Acknowledgements

APWA, AMWA, NACWA, and WEF would like to thank the following members and staff of their respective organizations who generously contributed to this publication by reviewing and commenting on early drafts. The experience and knowledge shared by these members was extremely valuable to the development of this publication, and is greatly appreciated.

APWA: Matt Singleton, Director of Public Works, City of Grapevine, TX; Joe Supreneau, Springfield Water and Sewer Commission, MA; Julia Anastasio, Senior Manager of Government Affairs, American Public Works Association

AMWA: Irene Caminer, Assistant Commissioner/Director of Legal Services, City of Chicago Department of Water Management, IL; Don Hawkes, Water Utilities Manager, City of Tempe, AZ; Carolyn Peterson, Director, Communications and Public Affairs, Association of Metropolitan Water Agencies

NACWA: Keith J. Jones, Divisional Deputy City Solicitor, Philadelphia Water Department, PA; Alexandra Dapolito Dunn, Former General Counsel, National Association of Clean Water Agencies; Nathan Gardner-Andrews, Counsel, National Association of Clean Water Agencies

WEF: Karen Pallansch and Cheryl St. Amant, Alexandria Sanitation Authority, Alexandria, VA; Daniel D. Clark, Bureau of Environmental Services, City of Portland, OR; James K. Sullivan, General Counsel, Water Environment Federation

Additionally, the sponsoring organizations would like to thank the following individuals at Dewey & LeBoeuf for their leadership and substantial work on this important project: Robert M. Andersen, Senior Counsel; Randall D. Benn, Partner; Deborah Koch, Senior Paralegal; Debra Sargent and Terri Howard, Administrative Assistants

September 2007

Background

The Nature of Terrorist Threats to Water Sector Infrastructure

Safety and reliability have always been important to water suppliers and wastewater treatment facilities, but following the attacks of 9/11, many owners and operators had to shift their focus to securing facilities against threats from terrorist attacks. Contingency and emergency response plans that were developed many years ago and designed to respond to major power outages or natural disasters such as flooding must now take into account a variety of possible security incidents that before 2001 appeared remote in the extreme. Most problematic for facility owners and security planners is the demonstrated willingness of terrorists to sacrifice their lives to achieve their deadly goal. The most prominent and likely means of terrorist attack on the water sector include the intentional release of chemical, biological, and radiological contaminants into the water supply or wastewater systems, disruption of service from explosions, and breaches in cyber security.

Most security experts believe that both drinking water and wastewater systems remain vulnerable to terrorist attack. A terrorist's goals in mounting an attack are to maximize the loss of human lives, cause as much economic loss as possible, strike at symbols of American life, and generally cause sufficient disruption in daily life to erode confidence in governmental and private systems. A successful attack on water sector infrastructure could accomplish these goals. The consequences of a successful attack include the potential loss of human lives, personal injury, and/or long-term illnesses; disruption of vital services for extended periods; overload of hospital and emergency response services; environmental and ecological damage; vast economic losses; and a loss of public confidence in the safety and quality of drinking water supplies, local wastewater treatment, and stormwater systems. This potential for loss of public confidence is a serious matter even in circumstances that do not result in major public health consequences.

Terrorist contamination of the water supply would have direct and immediate health consequences. Similarly, disruption of the local water supply can have devastating health and safety impacts, as the aftermath of Hurricane Katrina demonstrated. Terrorist attacks on a water supply system can have consequences for the attendant wastewater treatment system also. For example, flushing a drinking water distribution system in response to a chemical or biological attack and sending the resulting contaminated flows to the wastewater system or stormwater systems could overload, bypass, or disrupt the waste treatment process or impair stormwater systems. Unless the wastewater system can handle the volume, and effectively remove the contaminants, the contaminants could be discharged into receiving waters, ultimately causing large-scale environmental impacts.

Security threats to wastewater systems, while perhaps posing a less direct impact on public health, are nevertheless serious concerns. Chemical or biological contaminants added in relatively small quantities to a wastewater system could disrupt the treatment process. A direct physical attack on a wastewater collection system could create local public health

concerns and environmental impacts. Wastewater collection systems may also serve as conduits for malicious attacks by terrorists using explosives that could cause a large number of fatalities and injuries. An attack on a wastewater system could also create public health concerns if untreated wastewater were discharged to a river used as a downstream drinking water supply or to recharge aquifers utilized for drinking water purposes.

The National Academies of Science recently warned that threats to water sector security also raise concerns regarding cross-sector interdependencies of critical infrastructures: "Water utilities are largely dependent upon electric power to treat and distribute water. Likewise, electric power is essential to collect and treat wastewater, although diesel power generators can be used in the short term. The firefighting ability of municipalities would be seriously weakened without an adequate and uninterrupted supply of water, and intentional fires could be set as part of a terrorist attack to further exacerbate this impact. Explosive attacks in wastewater collection systems could affect other critical collocated infrastructures, such as communications."[1]

Preparation for, and response to, water sector security threats may be modeled after similar plans for natural hazards. Hurricane Katrina provided a tragic and costly lesson on the nation's state of readiness to respond to natural disasters that can cause both physical damage and contamination to water supply and wastewater treatment systems. The National Academies of Science and the Center for Disease Control also warn that an epidemic or pandemic illness could create failures in smaller water or wastewater utilities if those systems are disrupted due to incapacitation of essential personnel or absenteeism. Thus, threats from intentional attacks pose not only direct threats to the integrity of the nation's water sector, but also an array of other collateral consequences.

Nevertheless, sound security planning often serves the dual purpose of preventing, or preparing for, other contingencies, such as the threats of trespass and vandalism, or emergencies brought on by weather or other unexpected conditions. Preparing for, and securing systems against intentional acts of terrorism and vandalism mitigates the impacts from unavoidable natural disasters and heightens awareness of vulnerabilities of all kinds. Upgrading facilities in a manner that serves dual or multiple purposes may be the only economically feasible way to address security threats at many water sector facilities.

The Political and Legal Response to the New Threats

Political and legal responses to the 9/11 attacks were swift in the United States. Six weeks after the attacks, Congress passed what has been popularly referred to as the *USA Patriot Act*. 18 U.S.C. § 1 (2001). Following that Act and the subsequent establishment of the Department of Homeland Security (DHS), a number of sweeping safety and security reforms were passed. Many of those statutory reforms focus on the nation's critical infrastructure and mandate vulnerability assessments and subsequent corrective actions. *The Critical Infrastructures Protection Act of 2001*, 42 U.S. C. § 5195c, began the process of continuous national effort to ensure the reliability of physical and cyber infrastructure deemed critical to maintaining national defense, continuity of government, economic prosperity, and the quality of life in the United States.[2] The water sector was specified as "critical infrastructure" in the Act,[3] and the United States Environmental Protection Agency (EPA) was eventually designated as the lead federal agency to provide analysis, guidance, and leadership in responding to terrorist threats to water infrastructure. While major steps have been taken by EPA and owners and operators to protect drinking water supplies and wastewater treatment and collection systems (collectively referred to as the "water sector") from terrorist attack, the legal framework and the nation's security requirements are still evolving.[4]

EPA and DHS have responded to these and other warnings by publishing the 2007 Water Sector-Specific Plan (Water SSP) as input to the National Infrastructure Protection Plan.[5] The Water SSP outlines security goals and emergency response objectives for all water and wastewater utilities, government agencies, and other partners, and provides the overarching framework for integrating water sector critical infrastructure and key resource protection efforts into a unified program coordinated by DHS. The Plan takes important steps towards establishing security priorities and setting measures of success for security and emergency response programs within the water sector. It also consolidates, in one place, much of EPA's research, findings, and conclusions regarding the risk of terrorist attacks on the water sector and the tools for minimizing those risks and responding to attacks that do occur.

CHAPTER ENDNOTES

1 NRC, *Improving the Nation's Water Security: Opportunities for Research* at 8 (Feb . 27, 2007) (hereinafter cited as "NRC Report"). Strategically placed explosives are capable, in some cases, of disrupting the local water supply system, wastewater collection, and communications all at once if the conduits, cables, and other conveyance structures are collocated underground.

2 Id. at ∫ 5195c(b)(3).

3 Id. at ∫ 5195c(b)(2).

4 An early compendium of such laws is presented in GOVERNMENT INSTITUTES, HOMELAND SECURITY LAW HANDBOOK (ABS Consulting 2003). A legal compendium specific to the water sector is found in Environmental Law Institute, *Homeland Security and Drinking Water-An Opportunity for Comprehensive Protection of a Vital Natural Resource* (Oct. 2003). While these documents are good starting points for those who need background legal information, this Publication demonstrates that many applicable policies, security statutes, regulations, and judicial decision have already been added to legal framework since 2003.

5 U.S. Department of Homeland Security & U.S. Environmental Protection Agency, *Water: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan* (May 2007).

Chapter 1

The Federal Legislative Framework for Protecting Water Sector Infrastructure

The Federal Legislative Framework for Protecting Water Sector Infrastructure

A. The Safe Drinking Water Act Model for Mandatory Vulnerability Assessments Prepared by Water Suppliers

Though the vulnerability of our nation's water sector infrastructure was recognized before 2001, legislation that directly addressed the issue was not passed until after 9/11. The federal government's initial, pre-9/11 response to this vulnerability was President Clinton's issuance of a national security directive that designated "water systems" as vulnerable critical infrastructure.[6] In the days following the 9/11 terrorist attacks on the World Trade Center (WTC), a top priority for New York City was securing its water supply system. To do this, a team of engineers and lawyers from the United States Army Corps of Engineers immediately met with the FBI and officials from the State and City of New York to evaluate vulnerabilities in the City's drinking water system and implement interim measures to prevent contamination. Since then, terrorists have continued to strike infrastructure throughout the world—not only in Iraq and the Middle East, but also in Spain, England, and India. Therefore, effective legal and policy frameworks for security, improved security systems and emergency response plans, as well as constant vigilance, are demanded by all sectors of society.

After 9/11, Title IV of the *Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act)*[7] became the centerpiece federal legislation for the securing and protecting our drinking water systems. In particular, Title IV of the statute amended various aspects of the *Safe Drinking Water Act* (SDWA),[8] and imposed security related obligations on both community water systems[9] (CWS) and the Environmental Protection Agency (EPA).

Most importantly, each CWS was required to assess "the vulnerability of its system to a terrorist attack or other intentional acts [that are] intended to substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water."[10] With the help of guidance provided by EPA, each assessment was required to consider the vulnerability of the water supply source, the transmission, treatment, and distribution systems, and the risks posed to the surrounding community.[11] According to the statute, the assessment was to include:

> **A review of pipes and constructed conveyances, physical barriers, water collection, pretreatment, treatment, storage and distribution facilities, electronic, computer, or other automated systems which are utilized by the public water system, the use, storage, or handling of various chemicals, and the operation and maintenance of such systems.**[12]

The vulnerability assessments were completed and submitted to EPA on a rolling basis according to system size.[13] The largest systems (serving more than 100,000 people) were required to submit their assessments by March 31, 2003, medium-sized systems (50,000 to 99,999 persons served) by December 31, 2003, and the smallest CWSs covered by the amendments were to have submitted their vulnerability assessments to EPA by June 30, 2004.[14] Each CWS was required to incorporate the findings of its vulnerability assessment into the system's emergency response plan within six months.[15] With these submissions, completed under tight fiscal constraints, owners and operators of each CWS began the

process of prioritizing efforts to both secure their facilities and, at the same time, reduce the potential for civil liability.

The SDWA amendments passed as part of the *Bioterrorism Act* also imposed various obligations on EPA. These obligations generally are focused on protecting sensitive security-related information from disclosure, assisting CWSs in identifying the most likely threats to water systems and fulfilling their obligations under the statute, and conducting additional research and technical studies to enhance water system protections.[16] Such studies, currently in various stages of completion, were to address: (1) the prevention, detection, and response to the intentional introduction of contaminants to water sources and distribution systems; (2) methods by which terrorists could disrupt the availability or safety of drinking water supplies; and (3) methods by which alternative drinking water supplies could be utilized in the event of an attack on public water systems.[17]

The Water SSP serves in part as EPA's report on the progress it and this nation have made in meeting these statutory obligations since passage of the *Bioterrorism Act*. In its September 2002 Strategic Plan for Homeland Security, EPA established the following as its homeland security goal for water suppliers: "water utilities will incorporate security measures as a standard aspect of day-to-day operations and EPA, states, and tribes will review security measures at water utilities on a continuous basis." EPA and DHS recently expanded that goal by issuing a vision statement for the entire water sector as a part of the Water SSP referred to previously:

> **The Water Sector's Security Vision is a secure and resilient drinking water and wastewater infrastructure that provides clean and safe water as an integral part of daily life. This Vision assures the economic vitality of and public confidence in the Nation's drinking water and wastewater through a layered defense of effective preparedness and security practices in the sector.**[18]

DHS and EPA issuance of the Water SSP fulfilled many of the duties and obligations that the *Bioterrorism Act*, the SDWA, and the *Clean Water Act* placed on EPA and the federal government to begin leading the national effort to combat terrorism in the water sector.

The Water SSP comprehensively profiles water sector assets and systems in the United States, identifies federal, state, and local "security partners" within the sector, and establishes guidelines for effective relationships among those partners in preventing and responding to terrorism. It also assesses in some detail the known risks to the water sector from terrorism, and identifies the tools available for assessing those risks and responding to them effectively. Considerable attention is paid to the informational tools and communication systems available to combat terrorism. The Water SSP recounts the status of the critical infrastructure research—completed and ongoing—and establishes R&D priorities for the future. Finally, it lays out steps already taken to develop and implement protection programs for the water sector, while establishing goals for future progress in that critical area.

EPA also issued "Interim Voluntary Guidelines for Designing an Online Contaminant Monitoring System" on December 9, 2004, which contained guidelines that were prepared for the Agency by the American Society of Civil Engineers (ASCE), in cooperation with the American Water Works Association (AWWA) and the Water Environment Federation (WEF). The EPA Guidelines are a compendium of industry "best practices." Similarly, the Association of Metropolitan Sewerage Agencies (AMSA), now

NACWA, developed the aforementioned *Checklist*, an *Asset-Based Vulnerability Checklist for Wastewater Utilities*, and accompanying software to assist wastewater treatment agencies in assessing vulnerabilities to terrorism and other crisis events.

Although the EPA guidance was intended to be "voluntary," EPA maintains that failure to conform to applicable guidelines might subject an owner/ operator to tort liability in the event of an accident or a foreseeable incident. Therefore, such guidelines may have sway in the courts concerning what "reasonable" preventative measures include.[19]

Effective corrective actions in response to a vulnerability assessment can be as simple as upgrading physical security measures such as installing fencing, lighting and intruder detection equipment to prevent vandalism, securing storage of chemicals, and re-keying locks. On the other hand, such corrective measures can be as problematic as commencing employee security screenings or as technically challenging as securing an interconnected network of wastewater collection sewers. The cost of correcting problems identified in vulnerability studies can deter owners and operators from taking action.

ASCE has developed interim voluntary design standards to improve security at water and wastewater utilities that offer useful guidance both for security and non-security purposes, so-called "dual benefit" improvements. The design standards are specific to existing system designs. The American Water Works Association Research Foundation (AwwaRF) and the Water Environment Research Foundation (WERF) are developing a guidance document to address cyber-security at drinking water and wastewater utilities, applying lessons learned from other critical infrastructure sectors. Considering the importance of supervisory control and data acquisition (SCADA) systems to daily operations at many large utilities, these recommendations, if broadly and effectively implemented, could prove critical to securing the nation's water infrastructure.

The harsh experience of the airline industry demonstrates that remedial costs to an entire industry following an attack upon isolated airports or individual airlines can be many times greater than the costs of taking timely preventive measures against the attacks. Owners and operators ideally will consider all sources of funding before deciding not to institute corrective actions identified in a vulnerability study. Dual-benefit corrective actions significantly improve the likelihood of implementation of findings from a vulnerability assessment. For example, improved mitigation, recovery, and response capabilities often result in dual-benefits because such corrective action addresses threats from natural hazards (earthquake/ flooding) and intentional acts such as vandalism and terrorist events.

B. Legislative Developments Regarding Vulnerability Assessments for Wastewater Facilities

According to a 2006 Government Accountability Office (GAO) report[20] released on May 1, 2006, the municipal wastewater industry has over 16,000 plants that are used to treat a total flow on the order of 32,000 billion gallons per day (Bgal/d). EPA estimates that more than 92 percent of the total existing flow is handled by about 3,000 treatment plants that have a treatment capacity of 1 million gallons per day (Mgd) or greater, although more than 6,000 plants treat a flow of 100,000 gallons per day or less. Nearly all of the wastewater treatment plants provide some form of secondary treatment, and more than half provide some form of advanced treatment using a wide-range of treatment processes and configurations.

Thus, crafting a wastewater security strategy that is suitable for all wastewater treatment plants and collection systems is difficult.

Most water security experts believe that the chance of a terrorist attack at any given wastewater facility or collection system is remote. The GAO reported that wastewater utilities lag their water supply counterparts in security management, but have made significant improvements in recent years. Continued limited funding for such efforts, however, could impede further progress.

Federal law currently does not address wastewater security issues as comprehensively as it does drinking water security, and does not require vulnerability assessments. Nonetheless, the GAO reported that its survey of more than 200 of the largest wastewater plants in the United States found that many have made security improvements since the terrorist attacks of 9/11. The majority of the utilities surveyed indicated that they have completed, or intend to complete a plan to conduct some type of vulnerability or security assessment. In addition to these assessments, more than half the facilities responding to the GAO survey stated they did not use gaseous chlorine as a wastewater disinfectant, while others in the water sector believe that disinfectant alternatives to gaseous chlorine pose risks as well. Other security measures taken have generally focused on controlling access to the treatment plant through improvements in visual surveillance, security lighting, and employee and visitor identification. Less effort, however, has been made to address collection system vulnerabilities.

The majority of wastewater treatment owners or operators who chose to undertake a vulnerability analysis were driven primarily by a commitment to public service and risk management concerns, rather than legal requirements. However, once a vulnerability evaluation is undertaken, the information the wastewater treatment plant operator learns from its vulnerability assessment may put the operator on notice of dangerous conditions, which could give rise to additional civil or criminal liability if those conditions are not addressed.[21]

On April 26, 2006, EPA's Inspector General criticized that agency's efforts on security matters in general, reporting EPA needed more accountability in managing its plan to protect critical infrastructure, such as accountability applicable to managing the vulnerability plans of drinking water and wastewater facilities. The 2007 Water SSP goes a long way toward meeting those criticisms and providing for accountability in the future.[22]

Among the difficulties cited by wastewater utilities in securing facilities were the technical complexities and exorbitant expenses involved in safeguarding collection systems, specifically those that cover large areas and have many access points. Problems included not only the high cost of repair for wastewater infrastructure in general, but also other competing priorities that further contribute to budgetary demands on utility managers and operators.

On the heels of the GAO and EPA Inspector General's reports, the Senate Environment and Public Works Committee in 2006, approved a legislative plan to encourage cities and towns to assess the vulnerability of their wastewater treatment plants to terrorist attacks and natural disasters. Senate bill 2781, entitled *The Wastewater Treatment Works Security Act*, would have provided financial aid to utilities if they choose to do vulnerability assessments. The bill expressly authorized $220 million in EPA grants for wastewater security improvements: $200 million for grants to conduct vulnerability assessments and security enhancements; $15 million for technical assistance for small treatment plants; and $5 million

for refinement of vulnerability assessment methodology for treatment plants. A provision was added to the bill authorizing a training program to assist utilities in conducting assessments and in undertaking security enhancements. During committee deliberations, a competing bill was presented that would have also provided money for drinking water and wastewater treatment facilities that use chlorine as a disinfectant to convert to an alternative, such as sodium hypochlorite or ultraviolet light. The original provisions in Senate bill 2781 made it out of committee and onto the floor, but ultimately did not pass. This bill was reintroduced on May 3, 2007, as S.1303. It is essentially the same as the 2006 version, although it had not yet been enacted at the time this publication went to press.

Efforts in Congress have also focused on the chlorine issue. On March 19, 2007, representatives of the water sector met with members of Congress to discuss possible legislation governing chlorine gas. Prospective bills are expected to be similar to the previously introduced legislation, *The Community Water Treatment Hazards Reduction Act* (S. 2920), that called upon EPA and the DHS to identify high-risk wastewater and drinking water treatment facilities that use chlorine gas in their disinfection process. Under S. 2920, water sector facilities would be classified within three tiers, with Tier 1 [the highest classification of concern] including utilities that serve a population of greater than 100,000 people. Tier 2 includes utilities that cover a population of greater than 25,000 people but less than 100,000 people, and Tier 3 utilities cover a population with greater than 10,000 but less than 25,000 people. Once operators of these facilities are notified of their classification, they must conduct a feasibility assessment within 90 days on the viability of using inherently safer technologies, such as sodium hypochlorite. As this publication went to press, a new version of S. 2920 had yet to be introduced. There is still debate within the water sector over the ultimate risk of gaseous chlorine and the safety of other alternatives. Accordingly, utilities considering a change from chlorine should ideally weigh all their options and then make an informed choice.

Many in the water sector have taken the position that, first and foremost, the decision about whether to switch from chlorine gas to an alternative treatment technique should remain with the municipality itself. The factors in making the switch are complex, and include, but are not limited to, meeting the requirements of the *Clean Water Act*, ensuring public health, addressing affordability/cost concerns, and assessing the availability of alternative treatment options. Instead of the mandatory approach taken in S.2920, Congress has been encouraged by the water sector to take an incentives-based approach that recognizes the often complex, site-specific considerations that go into a decision regarding switching from chlorine gas.[23]

Congressional efforts also continue to support federal funding for security endeavors. For example, S.2920 sought to provide $125,000,000 per year for five years in grant funding. However, this funding level would be insufficient to make the upgrades that would be mandated relative to chlorine conversion at the thousands of drinking water and wastewater treatment facilities potentially covered by it. Changes

to the many unrealistic timeframes contained in S.2920 are also required because they simply would go unmet by both municipalities and the federal government and would open the door to unnecessary enforcement activity.

As this publication was being finalized, Congress continued its efforts to address security threats to the water sector. S.1968 was introduced on August 3, 2007, and would provide $245 million in grants over the next several years to help communities meet water and wastewater security needs. Progress on this bill remains uncertain.

Regardless of the outcome of the current legislation, vulnerability assessments and corrective actions at wastewater treatment facilities have already become standard practice for many facilities as noted by the GAO. The reasons that a wastewater treatment facility may wish to undertake a vulnerability analysis range from a commitment to safety and enlightened public service, to ordinary risk management concerns, to avoidance of potential civil liability. In an emergency situation, an owner and operator has only a brief time to react to a particular set of facts, or to decide whether it should communicate such facts to the public. A well thought out emergency response plan makes effective and timely decision-making in such situations possible.

The scope of remedial action in response to a vulnerability assessment may be governed by liability considerations stemming from state and local laws and, to some extent, judicial precedents. Many of these considerations are addressed in following sections of this publication. For all these reasons, vulnerability assessments ideally will be structured and undertaken with care.

The availability of tools for performing such assessments makes it possible to undertake such an assessment even if there is no heightened danger at a particular locale because it is secure, or because there is no known threat to it.

Some state laws and municipal ordinances mandate periodic risk management and security measures for publicly owned treatment works (POTWs). For instance, in some jurisdictions, such as Atlanta, Georgia, the general municipal ordinances have detailed policies regarding risk management assessment at all city operations. See, Atlanta City Code, Part 2, Art. VIII, §§ 2-1741-1746. Federal and state *Clean Water Act* requirements may contain provisions addressing risk management and security, as for example New York's State Pollutant Discharge Elimination System (SPDES) General Industrial Stormwater Permit, which, until recently, provided the following: "Facility security. Facilities shall have the necessary security systems to prevent accidental or intentional entry which could cause a discharge. Security systems described in the [Storm Water Pollution Prevention] plan shall address fencing, lighting, vehicular traffic control, and securing of equipment and buildings." Id., at Part III(D)(8).[24]

Even without a mandatory federal, state or local requirement that vulnerability assessments be conducted, many owners and operators have undertaken such assessments as a prudent step in an uncertain world. Such an assessment is the first step in protecting against civil liability as well.

CHAPTER ENDNOTES

6 Presidential Directive PD-63 (1998).

7 Pub. L. No. 107–188 (2002).

8 42 U.S.C. §§ 300f et seq.

9 As defined under the SDWA, CWSs are those systems serving at least 15 service connections or 25 residents year round. 42 U.S.C. § 300f (15).

10 42 U.S.C. § 300i-2 (a)(1). The EPA estimates that the United States has some 160,000 public drinking water systems, each supplying at least 25 persons or 15 service connections on a regular basis (EPA, 2004c). About one-third of this total number (53,000) are "community water systems," which serve cities, towns, mobile home parks, or residential developments. Most community systems are quite small, with 84 percent serving fewer than 3,300 persons each. "Non-community systems" are usually smaller, supplying individual schools, factories, campgrounds, or hotels, for example. The EPA estimates that about 107,000 non-community systems exist in the United States, although in aggregate, these small systems supply less than 10 percent of the U.S. population. Drinking water sources are also varied, from large surface water impoundments (reservoirs) or natural surface water bodies (e.g., lakes, rivers) to groundwater systems served by aquifers of varying complexity, interconnectedness, depth, and physical characteristics. NRC Report at 15.

11 See EPA Vulnerability Assessment Fact Sheet at 1 (Nov. 2002).

12 42 U.S.C. § 300i-2(a)(1).

13 See 42 U.S.C. § 300i-2(a)(2)(A)-(C).

14 Id. The security challenges and possible solutions for small sized water sector facilities are analyzed in detail in United States Environmental Protection Agency, *Drinking Water Security for Small Systems Serving 3,300 or Fewer Persons;* and Montana Water Center*, Protecting Public Health in Small Water Systems* (May 9-12, 2004)(Report of An International Colloquium).

15 42 U.S.C. § 300i-2(b). According to the amendments, "[t]he emergency response plan shall include, but not be limited to, 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 ... [and] shall also 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." Id.

16 See, e.g., 42 U.S.C. §§ 300i-2(a)(3)(nondisclosure of vulnerability studies); 300i-4(a) to (e) (threat evaluation and guidance on preventing terrorism); 300j-1 (research and technical assistance); 300i-2 (guidance to small public water systems); 300 i-3 (EPA development of methods to prevent, detect, and respond to chemical, biological, and radiological attacks). EPA's "Baseline Threat Report," completed in August 2002, contains information regarding the likely modes of terrorist attacks on water systems and, accordingly, is not publicly available.

17 42 U.S.C. §§ 300i-3; i-4.

18 U.S. Department of Homeland Security & U.S. Environmental Protection Agency, *Water: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan* (May 2007) at 33.

19 See note 26 and Section II. A. *infra*.

20 GAO, *Securing Wastewater Facilities: Utilities Have Made Important Upgrades but Further Improvements to Key System Components May Be Limited by Costs and Other Constraints* (GAO-06-390).

21 See Section II. *infra* regarding such liability and possible defenses available.

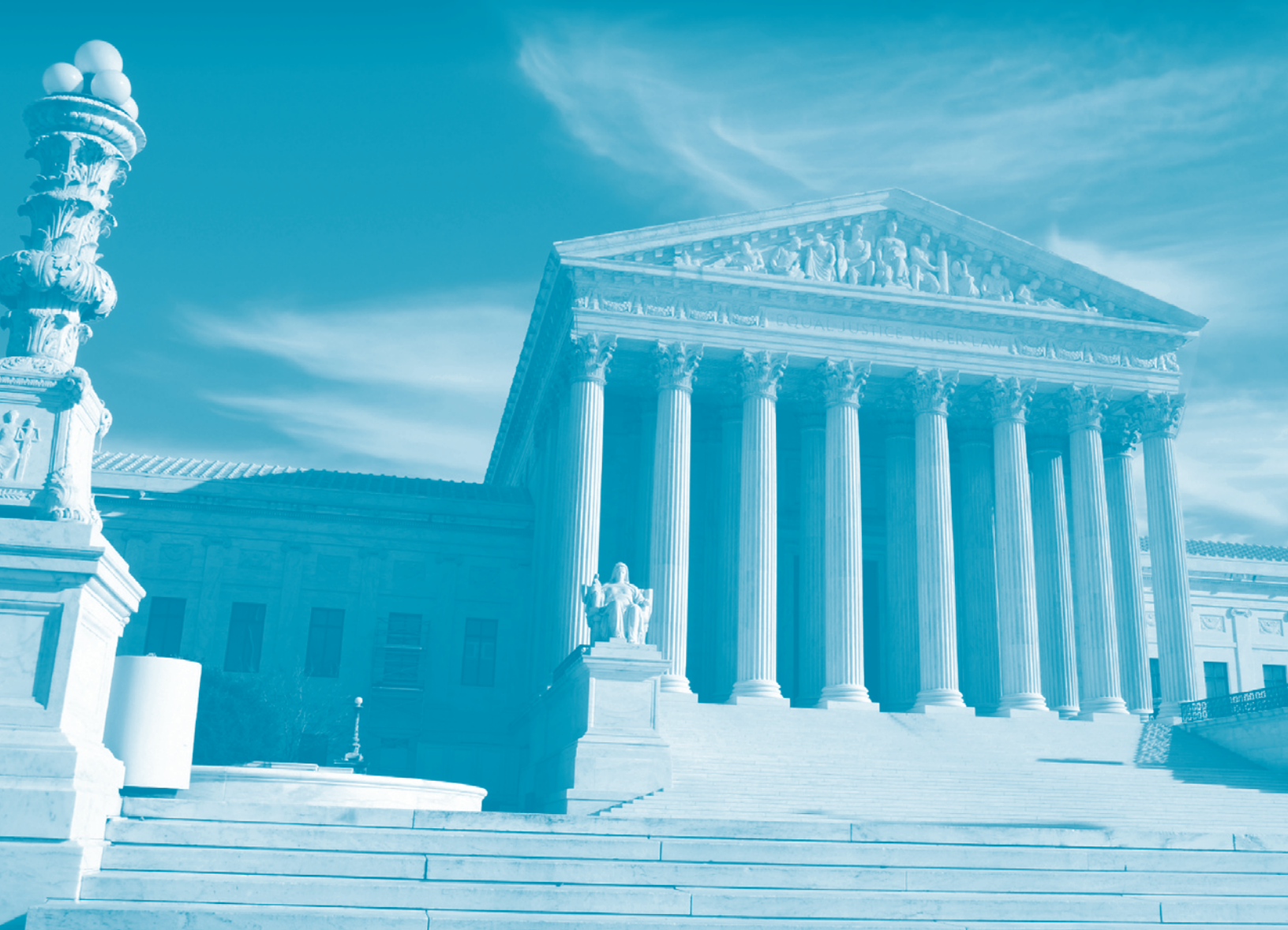
22 See text accompanying notes 6 and 18 *supra*.

23 Because the transport of chlorine gas or other potentially hazardous chemical disinfectant onto the water sector property presents an opportunity for terrorists to infiltrate the property and attack the facility, adequate security and access controls at the transporter's point of origin, along the truck route, and at the water sector facility are essential.

24 The New York SPDES General Permit for Stormwater Discharges Associated with Industrial Activity has been replaced by the SPDES Multi-Sector General Permit for Stormwater Discharges Associated with Industrial Activity. The SPDES Multi-Sector permit is modeled after USEPA's Multi-Sector Permit. The new permit does not mention risk management plans nor does it require any such plans to be implemented.

Chapter 2

The Duty to Protect the Public from Known or Foreseeable Terrorist Attacks and the Potential Civil Liability for Consequences of Terrorist Acts



The Duty to Protect the Public from Known or Foreseeable Terrorist Attacks and the Potential Civil Liability for Consequences of Terrorist Acts

A. Applicable Tort Principles of Due Care

Common law tort principles require owners and operators of water sector infrastructure to perform their general duties while acting in a "reasonable manner."[25] Stated another way, they should avoid acting negligently. The common law concept of negligence is the product of hundreds of years of litigation and judicial decisions. Negligence is conduct that falls below the standard established by law for the protection of others against unreasonable risk of harm.[26] Negligence occurs when harm is caused by owners and operators who fail to use "ordinary care," meaning the degree of care that would be used by those possessed of ordinary prudence or caution under the same or similar circumstances.[27]

The elements of negligence require plaintiffs in such cases to demonstrate that a duty is owed them; that the duty was breached; and that harm (damage) is caused by the breach of duty. The breach must also be the "proximate cause" of the harm.[28] For defendants to prevail, they must counter one of these elements, or prove that an affirmative defense exists. Normally, it is for a jury to determine how a reasonably careful owner and operator of water sector infrastructure should act under the circumstances, including before, during and following a terrorist threat or attack.

An owner or operator fails to act reasonably if they, or employees under their control, do something that a reasonably prudent facility operator would not have done under the circumstances. A failure to act reasonably can also occur by omission.[29] For example, failing to do something a reasonably careful facility owner or operator would have done under the same or similar circumstances would invalidate a defense of ordinary care. More specifically, if, as a result of a vulnerability study some action by a terrorist is reasonably foreseeable, failure to use reasonable means to prevent the harm may be actionable in tort.

The Terrorism Risk Insurance Act of 2002 (TRIA) creates an exclusive federal cause of action for any property damages, personal injury, or death arising out of or resulting from an act of terrorism as defined by the statute.[30] The federal action serves as the exclusive civil remedy for damages resulting from terrorist acts as defined under TRIA; however, the substantive tort law of the state in which the terrorist act occurred is to be applied by the federal court in determining liability for damages for loss of life and property.[31]

B. The Developing Case Law on Failure to Secure Facilities from Terrorist Attack

It is impossible to predict or prevent all forms of attack, and the courts will recognize that reality which is ever-present in the post-9/11 world. The law ordinarily only requires that reasonable measures be taken to protect customers and the public from those harms that can reasonably be foreseen and prevented. There are currently many foreseeable threats documented and known to the industry.[32] Government and private efforts to share information to thwart terrorism may have civil litigation consequences in the aftermath of an attack. Efforts by EPA to provide the water sector with methods to prevent, detect, and respond to

attacks,[33] and the establishment of the Water Information Sharing and Analysis Center (WaterISAC)[34] to coordinate the sharing of information regarding possible terrorist attacks have dramatically increased what water sector facilities know, and arguably can foresee, regarding future attacks.

The 1993 underground bombing at the World Trade Center (WTC) triggered tort actions in New York courts which raise the precise issue of what corrective actions must be taken when the risk of terrorist attack is identified in a vulnerability or risk assessment. Following the attacks of 9/11, numerous lawsuits were filed in New York for the deaths, injuries, and property damage sustained as a result of the attacks at the WTC. This section will address those cases and others. Taken together, the final results in the combined WTC cases will shape the law regarding what are reasonable actions to prevent terrorist attacks, as well as what are reasonable responses when such attacks occur.

For those owners and operators of facilities that have completed vulnerability studies, reasonable corrective actions should be considered a priority. Those without assessments should consider conducting them as soon as possible—particularly because the common law does not allow officials to plead ignorance of the facts as a defense in the event an incident occurs due to ignored threats (the so-called ostrich defense).

While precise court cases do not yet exist to tell us what "reasonable" security measures are required of a water sector facility to prevent or mitigate an attack, one can generally assess how the courts would view those issues in the future from landmark civil cases triggered by terrorist attacks outside the water sector. Vulnerability assessments are designed to assist in identifying problems and then taking reasonable steps to prevent attacks or accidents from happening. It can be legally risky to undertake a vulnerability study and not follow through on its findings. Taking reasonable corrective actions can be both sound policy and pose fewer legal risks because those actions both secure the system from preventable attacks, and potentially shield the owners and operators from legal liability if an incident subsequently occurs. What can be defined as "reasonable" corrective action in a particular case depends on the size, condition, and operations at the facility; therefore "reasonable" corrective action cannot be determined in a specific situation without the assistance of competent technical and legal advisors.

1. The First WTC Bombing Case—1993

In October 2005, the potential for litigation triggered by a "failure to secure" from terrorist attack became a reality. The jury decision in the *World Trade Center Bombing Case*,[35] opened the door for the individual plaintiffs to claim damages from the Port Authority of New York and New Jersey for the 1993 bombing of the World Trade Center (WTC) by terrorists. The civil case combined more than 400 claims for compensation (including those from families of the victims).

Broad warnings had been issued throughout the 1980s that the WTC could be a target for terrorist attacks. Local officials responded by engaging both internal and outside security experts to review the WTC's vulnerability to an attack. They recommended that the buildings' underground parking garage be closed to the public to prevent a bombing; however, no action was taken on this recommendation. On February 26, 1993, a van packed with explosives was detonated in the buildings' underground parking garage, killing six (6) people, and wounding more than 100. Property damage shut down the building for weeks. In March 1994, four terrorists were convicted of placing and detonating the bomb.

More than 175 civil lawsuits were also filed in the aftermath of the bombing. The plaintiffs contended that the Port Authority failed to implement security measures by, inter alia, keeping the parking garage open to the public, an action that resulted in a detonated bomb in the garage. As the owner of the buildings, the Port Authority sought to dismiss the lawsuits because the terrorist bombing was a criminal act that was not "foreseeable." However, the court disagreed and allowed the suits to go forward. In two rulings that are critically important for facilities that conduct vulnerability studies, the court noted that the Port Authority's own "eerily accurate" security reports had raised the specter of a vehicle bomb in the parking garage, so the attack was indeed foreseeable. Moreover, the court also rejected the Port Authority's claims of governmental immunity.[36]

Having cleared the way for the jury trial to proceed, a six-person jury, on October 26, 2005, ruled that the Port Authority didn't heed warnings by its own security consultants that the garage was vulnerable. The monetary damages would be decided in a separate proceeding. The final appeal and outcome of this litigation may impact a broad range of publicly and privately owned facilities considered "critical infrastructure," including both water suppliers and wastewater treatment facilities.

2. The WTC Cases Following the Attacks of 9/11

The civil litigation in the aftermath of 9/11 has the potential to both resolve, and further complicate, the issues regarding tort liability for damages suffered by individuals as a result of terrorist attacks. On the morning of September 11, 2001, suicide hijackers crashed airplanes into the World Trade Center Towers in New York City and the Pentagon in northern Virginia. After learning from phone calls of these hijackings and crashes, a passenger uprising on the fourth hijacked plane resulted in a crash in a Pennsylvania field. Following the crashes and the ensuing fires, the World Trade Center Towers collapsed.

The injured, and the representatives of the thousands who died from the terrorist-related aircraft crashes of 9/11, are entitled to seek compensation. Congress gave those victims of the terrorist-related aircraft crashes and their families a choice of remedy: they could enter the Victim Compensation Fund or file a traditional lawsuit, thus requiring claimants to choose between the two options.

By Act of Congress, they could seek compensation by filing claims with a Special Master established pursuant to the *Air Transportation Safety and System Stabilization Act of 2001*[37] (the ATSSS Act). If they chose to file a claim under the ATSSS Act, their claims were paid through a Victim Compensation Fund from money appropriated by Congress, within a relatively short period after filing. Claimants did not have to prove fault or show a duty owed on the part of any defendant. The amount of each individual's compensation for non-economic damages was limited to $250,000,[38] and economic damages were subject to formulas likely to be less generous than damage awards from individual lawsuits.[39] Additionally, compensation under the ATSSS Act and through the Victim Compensation Fund is contingent upon victims' families' waiver of their right to file, or be a party to, civil lawsuits for damages (either death or injury) resulting from the September 11, 2001 terrorist acts.[40] Moreover, punitive damages were unavailable.[41] The vast majority—approximately 98%—of the victims and their families chose to pursue compensation through the Fund and to forego litigation.[42] Because families must waive the right to pursue civil suits by participating in the Fund, fewer than 2% of the families opted either to file or join civil damages suits or not to file for any sort of compensation.

Rather than file under the ATSSS Act, victims had the option of seeking compensation in the traditional manner, by alleging and proving their claims in civil lawsuits, with the aggregate of their damages capped at the limits of defendants' liability insurance. ATSSS Act § 408(a). Section 408(b)(3) further provided that such actions were to be brought in the U.S. District Court for the Southern District of New York, as a matter of its "original and exclusive jurisdiction." The exclusive jurisdiction is to be "over all actions brought for any claim (including any claim for loss of property, personal injury, or death) resulting from or relating to the terrorist-related aircraft crashes of September 11, 2001." ATSSS Act § 408(b)(3). Section 408(b)(2) provided that the governing law for lawsuits is to be "derived from the law, including choice of law principles, of the State in which the crash occurred unless such law is inconsistent with or preempted by Federal law."

Fewer than ninety individuals,[43] including some of the injured and representatives of those who died, and ten entities[44] who all sustained property damage in the September 11, 2001 terrorist attacks, brought suit in Federal District Court against all of the following: defendant airlines, airport security companies and operators, an airplane manufacturer, and government defendants for what amounts to alleged failure to secure airports, individual airlines, and commercial buildings, such as the WTC, from terrorist attack. The case will produce specific law concerning the liability of operators and owners of the World Trade Center, that, by analogy, will provide guidance on the potential scope of liability to owners and operators in the water sector.[45] The "September 11th Civil Litigation"[46] is still ongoing.[47] Among the many issues involved are negligence claims against each of the defendants based on alleged failures to secure and protect against terrorist attacks. However, the decisions may be decided on New York state law grounds that do not easily translate to others states.

The ATSSS Act Victim Compensation Fund is also the remedy for victims and their families who were killed or injured as a result of the 9/11 terrorist-related plane crash into the Pentagon in Arlington, Virginia and the attempted hijacking resulting in the plane crash in Shanksville, Pennsylvania. Most of these victims' families entered the Fund, but some opted not to file with the Fund and initiated or joined their own lawsuits against the airlines, airport security companies, and other defendants.[48]

Thus far, the preliminary decisions from 9/11 litigation and other civil actions in the wake of terrorist attacks are consistent with the existing common law of torts in many other areas of governance and business activities. Most security law experts expect that a basic tenet of legal liability will emerge from the civil cases that could provide impetus for many owners of critical infrastructure, such as water suppliers and wastewater facilities, "to take reasonable steps to eliminate or mitigate a hazardous condition . . . [related to security inadequacies, once they are] made aware of a condition."[49]

3. Other Potential Liabilities for Failure to Secure against Terrorist Attacks

Once a vulnerability evaluation is undertaken, the information the plant operator derives from the vulnerability assessment may put the operator on notice of dangerous conditions, which could give rise to other civil or criminal liabilities if those conditions are not addressed. Individual and corporate criminal liability have been known to attach to certain failures to act on knowledge necessary to protect the public.[50] Generalized warnings of terrorism against all water related utilities "could be considered notice that a hazardous condition may potentially exist. Once a vulnerability assessment is complete, the resulting recommendations also could be considered as notice of a dangerous condition. These forms of warnings and notice could potentially result in liability if the recommendations are not addressed."[51]

With respect to potential criminal liability, a post-audit failure to correct an identified problem arguably can show either a knowing or deliberate indifference to a violation, either of which can be construed as criminal intent. It may even introduce the possibility of individual liability. See, e.g., *U.S. v. Ming Hong*, 242 F.3d 528 (4th Cir.), cert. denied, 534 U.S. 823 (2001). In one relevant environmental case, a shipping company was held criminally liable when a ship captain reported problems with leaking tanks to management, but the company failed to correct the problem. *United States v. Polembros Shipping Ltd.*, No. 00-0534 (N.D. Cal. 2000).

Failure to protect against known or reasonably ascertainable terrorist-related hazards can also result in negligence liability for employers under theories of negligent hiring, retention, supervision and/or training, and under premises liability and vicarious liability. If, for example, a terrorist attack would focus upon access to a facility's chlorine tanks, and a teenage trespasser gains access instead, and causes the harm, liability in tort could be found in most states if appropriate corrective action has not been taken. Another example of a foreseeable threat to water infrastructure is an attack on the water supply resulting in contaminated water being released into the wastewater system as an emergency response measure. Also, damage to a utility or wastewater collection system could similarly prevent water from being properly treated, negatively impacting in-stream water quality and water intakes downriver, resulting in dangerous environmental damage. Individual and corporate criminal liability may also attach to certain failures to act on knowledge that could protect the public.[52] Generalized warnings of terrorism against all water related utilities "could be considered notice that a hazardous condition may potentially exist. Once a vulnerability assessment is complete, the resulting recommendations also could be considered as notice of a dangerous condition. This notice could potentially result in liability if the recommendations are not addressed."[53]

A "knowing or reckless failure" to correct security vulnerabilities may also subject the individuals and entities to criminal prosecution. The importance of acting promptly upon knowledge pertaining to existing hazards at water resources facilities is illustrated by an incident in Bethlehem, Pennsylvania.[54] In July of 1993, the City of Bethlehem hired a consultant to study the lab at the City's wastewater treatment facility. The consultant's report found that tests on weekends, as required under federal regulations, were not being conducted.

Officials at the wastewater treatment facility sought additional employees and funds to conduct the required tests. In the meantime, employees concealed the violations in self-monitoring reports submitted to the state and EPA. In April 1994, an inspection by EPA discovered that tests were not being conducted in accordance with EPA regulations. Moreover, during the EPA's investigation, it discovered that city officials did not correct the facility's testing methods for nearly a year after learning of the deficiency.

Following EPA's discovery, the City immediately corrected the violations. However, because of the City's failure to take action between the time of the consultant's report and the discovery of the violations by EPA, the agency commenced criminal investigations against the City and certain employees.

C. Statutory Defenses to Negligence Suits for Failure to Protect

Governmental immunity is a defense that may shield public water suppliers, POTWs, and their owners and operators from liability for failure to secure the facilities. Immunity creates an absolute bar to certain suits against state and local governmental entities, but is not available to private owners and operators of water sector infrastructure. Thus, in determining whether any immunity is available under state law, the first step is to determine the status of the facility as public or private.

In many states, immunity against negligence suits exists for publicly owned collection and treatment systems and water suppliers, but is limited to circumstances that are specifically enumerated in the relevant statutes. In other states, however, municipal water suppliers and POTWs have blanket immunity under state tort claim acts, which are often modeled after the *Federal Tort Claim Act*. In such states, unless conduct falls into a category of situations where immunity does not apply—such as gross negligence or a knowing/reckless failure to protect—a publicly owned facility is not liable for negligence.

The case of *In Re World Trade Center Disaster Site Litigation*, 456 F.Supp. 520 (S.D. N.Y. 2006), will ultimately decide whether a city and its agencies have immunity under New York law for harms caused by the terrorists' attack on the WTC. Enacted in 1951, at the height of the Cold War, the *New York State Defense Emergency Act* (SDEA) provides for a comprehensive response to attacks upon the United States, and the State of New York, by coordinating the private and public sectors to "make possible the recovery of the people and the rehabilitation of the economic and social life of the state following any such attack." N.Y. Unconsol. Law SDEA § 9102-a (McKinney 2006). See also *7 WTC*, 2006 U.S. Dist. LEXIS 749, 2006 WL 62019 at *6. *Daly v. The Port Authority*, 7 Misc. 3d 299, 793 N.Y.S.2d 712 (N.Y. Sup. Ct. 2005). In the interest of ensuring that public and private entities will work aggressively to prepare for, and respond to, attacks, the SDEA provides immunity for actions taken "in good faith carrying out, complying with or attempting to comply with" any law or order requiring such a unified response and relating to "civil defense." SDEA § 9193. See also *7 WTC*, 2006 U.S. Dist. LEXIS 749, 2006 WL 62019 at *6.

The City defendants in the WTC litigation, the Port Authority, and other named defendants assert that all actions they took in response to the attacks were taken in good faith, to comply with the Declarations of Emergency issued by the President, the Governor, and the Mayor, that all actions related to the "civil defense," and thus their actions fall within the express grant of immunity provided by the SDEA. The immunity issue is now before the Second Circuit for decision.[55]

D. Alternative Tort Theories of Civil Liability: Ultrahazardous Activity

If an act of terrorism or vandalism at a water supply system or wastewater treatment system causes injury resulting from a release of chlorine or other disinfectant chemicals, a plaintiff might allege that the agency is strictly liable on the theory that the storage of toxic chemicals is an "ultrahazardous activity." See 3 Restatement of Torts (Second), Torts, § 520. In some cases, the outcome would be determined by a state's sovereign immunity statute. For example, in Colorado, there is a statutory prohibition against the imposition of strict liability in connection with public water or sanitation facilities. Colorado Rev. Statutes 24-10-106(4). If no such prohibition exists, a court might weigh the factors identified in the Restatement of Torts: existence of a high degree of risk; likelihood of great harm; inability to eliminate the risk through reasonable care; extent to which the activity is not one of common usage; inappropriateness of the activity to the place in which it is carried on; and the extent to which the activity's value to the community is outweighed by its dangerous attributes. Id. At least one court weighed these factors and concluded that the storage of hazardous chemicals was not an ultrahazardous activity. See *French Putnam LLC. v. County Environmental Services et al.*, 2000 WL 1172341, *15.

CHAPTER ENDNOTES

25 Restatement Second of Torts, § 283.

26 Restatement Second of Torts, § 282 . Negligence per se involves a duty that is imposed by statute or regulation. Id. at §§ 285-86; 288. When a statute or regulation imposes a clear duty on a facility, it can create a boundary which defines ordinary care for every covered facility. Tort law treats violations of such standards as negligence per se. Negligence per se does not flow from every statute or regulation. If the courts adopt them as a standard of ordinary care, the violation of that standard may be considered as evidence of negligence and will result in liability unless the defendant has a legal excuse for violating the law. For example, if a water supplier failed to conduct a vulnerability study as required by *Title IV* of the *Bioterrorism Act*, and a terrorist incident occurred at that plant, the court could hold such failure to be negligent per se. Id at § 283. For an in-depth survey of one State's (Pennsylvania) tort and property laws, and their potential application to a terrorist attack at a water supply system, see Robert M. Andersen & Carl R. Shultz, *Legal Liability of Water Systems for Terrorist Induced Harm*, In "Post 9-11 Water System Security and Liability" (American Water Works Ass'n, Pennsylvania Section, March 24, 2005).

27 Restatement Second of Torts, § 283. In the security context, the duty is to act in a manner that reasonably protects others. Restatement Second of Torts, § 314. For an analysis of negligence applied to water supply facilities, *see, e.g.*, Joseph T. Bockrath, *Liability of Water Supplier for Damages Resulting from Furnishing Impure Water*, 54 A.L.R. 3d 936 (2004).

28 Id. at § 435 (legal or proximate cause).

29 Restatement Second of Torts, § 284(b).

30 For a full discussion of insurance against terrorist acts, see Section VII *infra*.

31 See id.

32 *See* U.S. Department of Homeland Security & U.S.Environmental Protection Agency, *Water: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan* (May 2007) at 45-59; Background : The Nature of Terrorist Threats to Water Infrastructure, supra, at pages 3-5. Foreseeability of a threat is required to prove proximate cause. Restatement Second of Torts at § 435 (legal or proximate cause). *See generally*, Comment: *Foreseeable Change: The Need for Modification of the Foreseeability Standard in Cases Resulting from Terrorist Acts After September 11th*, 74 UMKC L. Rev. 165 (2005).

33 300i-4(a) to (e).

34 The WaterISAC is addressed in detail in the sections regarding security information. See, Section IV (E), *infra*.

35 *The World Trade Center Bombing Litigation*, 3 Misc. 3d 440, 776 N.Y.S.2d 713 (N.Y. S.Ct. 2004)(Index No. 600000-1994), affirmed, 13 A.2d. 3d 66, 784 N.Y.S.2d 869, 2004 N.Y. App. Div. LEXIS 14720 (App. Div. 1st Dep't 2004), reargument denied by, 2005 NY App Div LEXIS 2120 (1st Dept, Feb. 24, 2005). The jury verdict on liability was issued on Wednesday, October 26, 2005. Anemona Hartocollis, "Port Authority Seeks Voiding Of Jury Verdict," New York Times, p. 2 (December 7, 2005). On March 2, 2007, the court refused to set aside the verdict. Anemona Hartocollis, "Judge Refuses to Set Aside Ruling in '93 Bombing Case," New York Times, p. 5 (March 3, 2007). The case is ongoing and appeals are likely.

36 *Id.*

37 Pub. L. No. 107-42, 115 Stat. 230 (2001) (codified at 49 U.S.C. § 40101). *See generally* Marshall S. Shapo, *Compensation for Terrorism: What We Are Learning*, 53 DePaul L. Rev. 805 (2003).

38 *See* September 11th Victim Compensation Fund of 2001, http://www.usdoj.gov/archive/victimcompensation/distribution_plan_example.html.

39 *See* Elizabeth Berkowitz, *The Problematic Role of the Special Master: Undermining the Legitimacy of the September 11th Victim Compensation Fund*, 24 Yale L. & Pol'y Rev. 1, 24-30 (2006) (discussing the shortcomings of the Fund for victims' families).

40 See James P. Kreindler & Brian J. Alexander, *September 11 Aftermath: A Perspective on the VCF and Litigation*, 18 Air & Space Law 1 (2004). Congress passed the ATSSSA Act with the purpose of protecting the airline industry from massive civil lawsuits and bankruptcy. See note following 49 U.S.C. § 40101. Further, the Act established the Victim Compensation Fund to process victims' damage claims efficiently and quickly compensate the families for their losses. *See* Kenneth R. Feinberg, *Final Report of the Special Master for the September 11th Victim Compensation Fund of 2001* 3, http://www.usdoj.gov/final_report.pdf.

41 ATSSSA, § 405(b)(5).

42 Kenneth Feinberg, the Special Master of the Victim Compensation Fund, reports in his closing statement regarding the Fund that "[o]ver 98% of eligible families who lost a loved one voluntarily decided to participate and submitted claims to the Fund." Kenneth R. Feinberg, *Closing Statement from the Special Master*, Mr. Kenneth R. Feinberg, on the *Shutdown of the September 11th Victim Compensation Fund*, http://www.usdoj.gov/archive/victimcompensation/closingstatement.pdf.

43 Betsy J. Grey, *Homeland Security and Federal Relief: A Proposal for a Permanent Compensation System for Domestic Terrorist Victims*, 9 N.Y.U. J. Legis. & Pub. Pol'y 663 (2006) ("Fewer than ninety people ultimately decided to opt out of the September 11th Fund and sue the airlines and other defendants." (citing Kenneth R. Feinberg, What is Life Worth? 164 (2005))).

44 In re September 11 Litigation, 280 F. Supp. 2d 279, 287 (S.D.N.Y. 2003).

45 Cases alleging wrongful death and personal injury as a direct result of circumstances leading up to and including the terrorist acts of September 11, 2001 have been consolidated for pre-trial proceedings as *In re September 11 Litigation*, 21 MC 97 (AKH). Cases alleging property damage as a direct result of the plane crashes have been consolidated as *In re September 11 Litigation*, 21 MC 101 (AKH). See discussion infra, Part III.A for an overview of the consolidated cases based on personal injury as a result of related events subsequent to the plane crashes.

46 *In re September 11 Litigation*, 280 F. Supp. 2d 279 (S.D.N.Y. 2003) (Motion for Interlocutory Appeal denied by *In re September 11 Litigation*, 2003 U.S. Dist. LEXIS 17105 (S.D.N.Y. Oct. 1, 2003), affirming the earlier denial of Defendants' Motion to Dismiss, *In re September 11 Litigation*, 2003 U.S. Dist. LEXIS 16351 (S.D.N.Y., Sept. 19, 2003)).

47 See *In re September 11 Litigation*, 2003 U.S. Dist. LEXIS 16351 (Sept. 19, 2003); *In re September 11 Litigation*, 2003 U.S. Dist. LEXIS 17105 (Oct. 1, 2003). Judge Alvin K. Hellerstein, U.S. District Judge in the Southern District of New York, oversees all September 11 litigation cases, including "[c]ases involving claims arising out of, resulting from, or relating to the terrorist-related aircraft crashes of September 11, 2001 and naming an airline, an airport security company, and/or The Port Authority of New York and New Jersey . . . ." Information for Counsel in September 11 Litigation, United States District Court, Southern District of New York, http://www1.nysd.uscourts.gov/cases.php?form=sept11. Following the Second Circuit decision in *McNally v. The Port Authority (In re WTC Disaster Site)*, 414 F.3d 352 (2d Cir. 2005), which held that post-9/11 clean-up workers' respiratory injury claims based on their exposure to the air around the WTC shortly after September 11 "result from and relat[e] to" the September 11, 2001 terrorist-related air crashes specifically delineated in the ATSSSA Act, those claims were incorporated into Judge Hellerstein's September 11 docket, under the caption 21 MC 100 (AKH). See discussion *infra* Part III.A.

48 See Lawrence Hurley, *A Day Before Deadline, Some Families of 9-11 Victims Decide to Sue,* The Daily Record (Baltimore), Jan. 21, 2004, available at http://findarticles.com/p/articles/mi_qn4183/is_20040121/ai_n10059459 ("Other factors also prompted [plaintiff's attorney Keith S.] Franz to advise his clients to litigate, including the plaintiff-friendly wrongful death statute in Virginia and the fact that—unlike in Manhattan—there will be no property claims because the U.S. government has decided not to sue for the damage caused to the Pentagon.").

49 Interim Voluntary Security Guidance for Water Utilities, § 1.2.2.2 (2004). See also Checklist at p. 2.

50 See, e.g. U.S. v. *Ming Hong*, 242 F. 3rd 528 (4th Cir. 2001), cert. den. 534 U.S. 823 (2001); *United States v. Polembros* Shipping Ltd., No. 00-534 (ND Ca. 12/19/2000).

51 Interim Voluntary Security Guidance for Water Utilities, § 1.2.2.2 (2004).

52 See, e.g. *U.S. v. Ming Hong*, 242 F. 3rd 528 (4th Cir. 2001), cert. den. 534 U.S. 823 (200); *United States v. Polembros Shipping Ltd.*, No. 00-534 (ND Ca. 12/19/2000).

53 Interim Voluntary Security Guidance for Water Utilities, § 1.2.2.2 (2004).

54 These facts are excerpted from articles on September 27, 1997, August 2, 1997 and April 24, 1997 in Morning Call (Allentown, PA), which are available online at: http://www.mcall.com/.

55 The case is discussed in detail in the section on employer duties to employees, Section III *infra*.

Chapter 3

Particularized Duty to Employees Regarding Terrorist Threats and Attacks

Particularized Duty to Employees Regarding Terrorist Threats and Attacks

In addition to the general common law duty to the public at large to secure a facility from reasonably foreseeable terrorist threats, employers are specifically responsible under both statutory and common law requirements to protect their workers. First responders have filed suit in New York State Court and federal court against the City of New York under tort law and state statutory laws related to worker protection and compensation statutes. Those cases will go a long way toward establishing legal standards for the protection of those classes of government employees and contractors who must respond to terrorist attacks.

A. The World Trade Center Disaster Site Litigation

Following 9/11, state court cases were also brought by City workers, including police, firemen, rescue workers, demolition experts and other employees who were first responders. They alleged that they had sustained respiratory injuries in their complaint against the City of New York, the Port Authority of New York and New Jersey, and City contractors who were engaged to demolish, cart away and clean up the debris of the destroyed buildings. The cases were consolidated in state court for pre-trial proceedings as *In re World Trade Center Disaster Site Litigation*, 21 MC 100 (AKH). Although the complaints initially were exclusively based on New York worker protection and compensation laws, they were subsequently removed by the City and other defendants to the Federal District Court for the Southern District of New York to address questions under the ATSSS Act.

As an initial matter, the District Court had to decide if the case was properly removed, or should be remanded to state court. *In re World Trade Center Disaster Site Litigation* ("Hickey"), 270 F. Supp. 2d 357 (S.D.N.Y. 2003), rev'd, *McNally v. Port Auth. (In re World Trade Center Disaster Site Litigation)*, 414 F.3d 352, 371 (2d Cir. 2005) (reversed District Court decision, in part on immunity and preemption grounds), *on remand*, *In re World Trade Center Disaster Site Litigation*, 456 F. Supp. 520 (S.D.N.Y. 2006). Among the preliminary questions addressed was whether or not workers at the site who alleged injury had to bring any action in federal court under the ATSSS Act because it was a "claim (including any claim for loss of property, personal injury, or death) resulting from or relating to the terrorist-related aircraft crashes of September 11, 2001." ATSSSA § 408(b)(3).

The District Court had previously decided that construction workers who had been injured in the course of their demolition and clean-up work at the World Trade Center site could maintain state court actions and held that the scope of preemption provided for by § 408 of the Act did not cover their injuries. Those cases were remanded to New York state court. See *Graybill v. City of New York*, 247 F. Supp. 2d 345 (S.D.N.Y. 2002), and *Spagnuolo v. Port Auth. of N.Y. and N.J.*, 245 F. Supp. 2d 518 (S.D.N.Y. 2002). The District Court held that Congress did not intend to oust state court jurisdiction in cases involving injuries common to construction and demolition sites generally, such as those sustained by the plaintiffs when they were struck by objects at the site. "Although the dangers and pressures of the WTC site may have been greater than most normal construction sites, there was neither argument nor allegation that the accident that resulted in plaintiff's injury was unique to that site or that situation." *Graybill*, 247 F. Supp. 2d at 351. The court specifically reserved judgment on whether the Act confers federal jurisdiction in cases brought by plaintiffs alleging risks and duties that could be considered particular to the

conditions caused at the World Trade Center site as a result of the September 11 aircraft crashes.

The District Court specifically held that the claims of plaintiffs alleging respiratory injuries caused by exposure to contaminants in the demolition and clean-up efforts at the World Trade Center site, up to and including September 29, 2001, "arise out of, result from, and are related to the terrorist-related aircraft crashes," are governed by federal law, and are exclusively within the jurisdiction of this court pursuant to § 408 of the Act. Claims arising from exposure after September 29, 2001, or at sites other than the World Trade Center, must be remanded to the New York state court. *Hickey*, 270 F. Supp. 2d at 379.

The Second Circuit agreed with those portions of the District Court decision which refused to remand actions to New York state court, but noted that it saw no basis for the District Court's ruling that the ATSSS Act's preemptive effect differs depending on whether the respiratory injuries were suffered at the World Trade Center site or elsewhere, or on whether those injuries were suffered before or after midnight on September 29:

> **Nothing in the language of the statute or the legislative history suggests such lines of demarcation. The district court's geographical line would mean that, as to a given pile of debris that gave off toxic fumes both at the World Trade Center site and at a marine transfer station or the landfill to which it was transported, the claim of a worker who inhaled those fumes at the World Trade Center site would be preempted, while the claim of a worker who inhaled fumes from the same debris at either of the other sites would not. And given that it was December or later before all of the fires caused by the crashes were extinguished, the district court's cutoff date would mean that ATSSSA preempts the claim of a worker who inhaled smoke from a fire on September 29 but not the claim of a worker who inhaled smoke one day later from the same fire. We cannot conclude that Congress intended such differences. 414 F.3d at 380.**

The Second Circuit sent the case back to the District Court for reconsideration of its state court remand decisions in light of the Circuit's instructions. Plaintiffs subsequently amended their complaints to include claims for negligence, and wrongful death. *In re World Trade Center Disaster Site Litigation*, 456 F. Supp. at 542. The City and other Defendants continued to argue that they were immune from suit based upon state and federal law, and moved for dismissal of the cases. The court held that more facts were necessary before it could rule on the immunity issues. Id. at 575. It refused to grant a motion for interlocutory appeal on the immunity issue, a decision which the appellate court recently reversed, finding that immunity as a threshold issue should be decided before proceeding with the trial. *In re World Trade Center Disaster Site Litigation*, 2007 U.S. App. LEXIS 8728 (2d Cir. Mar. 9, 2007). It should also be noted that workers compensation benefits have, in some states, been held to preempt employees' negligence claims where injury occurred while on duty or in the workplace.

Assuming all of the major federal cases involving injuries sustained as a result of the 9/11 attacks, both on the day of the attack and subsequently, result in final decisions on the tort issues, those decisions will in all likelihood serve as a model for all future tort litigation generated by terrorist attacks. In addition, they will provide needed guidance for the water sector regarding what constitutes negligent failure to secure a facility from future attacks, how to avoid such liability, and whether state and federal immunity shields POTWs and public water suppliers from terrorist related tort and property liability.

B. The Occupational Safety and Health Act and State Workplace Safety Statutes

The 9/11 attacks raised specific questions about airport security, aircraft safety, and WTC building vulnerabilities that affect those individuals who worked at the affected facilities on a daily basis. While mostly focused upon the airline industry, questions were also raised about WTC design and safety features that illuminate concerns for workplace safety in general.

These worker issues related to terrorist attacks have been further underscored by the subsequent anthrax attacks, the potential for a pandemic flu virus, concern for the alleged availability of the smallpox virus, and other potential terrorist or natural threats to the personal well-being of employees in other workplaces, including those in the water sector.

The Occupational Safety and Health Act (OSHA Act), 29 U.S.C. §§ 651-678, is the comprehensive federal statutory scheme designed to assure working individuals in the country a safe and healthful working environment. OSHA, however, does not apply to "any State or political subdivision of a State." 29 U.S.C. § 652(5). It is not clear whether municipal water supplier or wastewater authorities are exempt as "political subdivisions". They may be subject to OSHA liability unless they meet the test of a "political subdivision" which has been defined to include any entity that is:

> (1) **"created directly by the State, so as to constitute a department or administrative arm of the government" or**
>
> (2) **"administered by individuals who are controlled by public officials and responsible to such officials or to the general electorate."**
>
> 29 C.F.R. § 1975.5(b).[56]

At least one federal court has held that a municipal water department was a "political subdivision" exempt from federal labor-relations laws. See *Manfredi v. Hazelton City Authority, Water Department*, 793 F.2d 101 (3rd Cir. 1986) (interpreting the use of "political subdivision" under the LMRA and the NLRA); *Brock v. Chicago Zoological Society*, 820 F.2d 909, 910 (7th Cir. 1987) (noting that the interpretation of "political subdivision" under the NLRA "offer[s] authoritative guidance" to its interpretation under the OSHA Act).

Although municipal employers may be exempt from the federal OSHA, more than twenty states have enacted laws which are patterned on the requirements of OSHA and that extend to public and private employees within those states. Thus, it is useful to review the requirements of OSHA's "general duty clause" in light of the events since 9/11.

The OSHA Act's general duty clause, 29 U.S.C. § 654(a), requires that employers furnish a place of employment that is "free from recognized hazards that are causing or are likely to cause death or serious physical harm" to employees. The Occupational Safety and Health Administration (OSHA) normally issues citations under the general duty clause when four elements are present: (1) the employer failed to keep his/her workplace free of a hazard to which employees were exposed; (2) the hazard was recognized either by the employer specifically or by the employer's industry generally, or was so obvious that common-sense recognition should have occurred; (3) the hazard was causing or likely to cause death or serious physical harm; and (4) there was a feasible means available that would eliminate or materially reduce the hazard.

In the past, OSHA has used the general duty clause to address problems as varied as workplace violence, finding that in workplaces where the risk of violence and serious personal injury are significant enough to be recognized hazards, the general duty clause would require the employer to take feasible steps to minimize those risks. On the other hand, OSHA has stated that violence that represents "random antisocial acts which may occur anywhere" would not subject an employer to a general duty clause citation.

Enforcement under the general duty clause thus relies on a fact-specific, case-by-case inquiry. Whether situations such as vandalism or terrorism could lead to an enforcement action will depend on whether there are clear hazards that can be feasibly addressed, in which case enforcement under the general duty clause is more likely, or whether the situation is more of a random, unforeseeable act, in which case enforcement is less likely. In the case of potential anthrax contamination through the mail, for instance, the OSHA Act's general duty clause suggests that employers would be well-advised to assess the risk of employee exposure and the feasibility of addressing any exposure concerns, considering such factors as whether the facility has its own mailroom and mailroom employees, the type of mail that is processed, the facility's proximity to any known anthrax outbreaks, and the extent to which increased security may address potential problems. In November 2001, OSHA prepared a guidance document on how businesses can voluntarily assess their risk for anthrax and take appropriate precautions.[57]

In the wake of 9/11, the OSHA also has updated its publication *How to Plan for Workplace Emergencies and Evacuations,* which outlines the steps employers should take in preparing emergency action plans. Water resources facilities may wish to examine this publication as they review their crisis management procedures. In addition to the general duty clause, water resources facilities may be subject to OSHA's Process Safety Management Standard, which requires "process hazard assessments" and related actions to prevent or minimize accidental workplace releases of substances including anhydrous ammonia and chlorine. See 29 C.F.R. § 1910.119. The standard applies to processes that involve listed chemicals above specified threshold quantities; the threshold for anhydrous ammonia is 10,000 pounds and the threshold for chlorine is 1,500 pounds. A process is any activity including any use, storage, handling, or on-site movement. Employers covered by the rule must compile written process safety information and perform process safety analyses. Employers also must implement written operating procedures that provide clear instructions for safely conducting activities involved in each process covered by the rule. Employees involved in operating a covered process must be provided with training. New or modified facilities are subject to a pre-startup safety review, and the ongoing integrity of process equipment (such as tanks and piping systems) must be maintained. Employers must investigate incidents that result in, or reasonably could have resulted in, a catastrophic release of a highly hazardous chemical in the workplace, and must establish emergency action plans.

A number of states and municipalities have statutes and/or regulations designed to serve the same purposes as the federal OSHA Act--establishment and maintenance of a comprehensive occupational safety and health management program. Such programs are designed to provide a safe and healthful work environment for employees. In addition, municipal employers, like other employers, can be held liable under various negligence theories for violations of common law duties to maintain a safe working environment.[58] Failure to protect against known or reasonably ascertainable hazards can result in negligence liability for employers under theories of negligent hiring, retention, supervision and/or training, premises liability and vicarious liability.

As a general matter, employees are informed of their rights in this regard. Municipal employers should consult local laws and regulations to determine what affirmative workplace safety components are required and the penalties associated with non-compliance. Employers can be held liable in a civil action brought by employees who are injured for violations of OSHA regulations pursuant to a negligence per se standard,[59] or pursuant to an established common law duty to maintain a safe working environment. Although there are not yet any across-the-board new requirements that employers undertake affirmative additional measures for workplace safety in light of terrorist threats, numerous employers, in response to recent events, are reexamining and adjusting internal policies governing such things as building security, mail access, and foreign travel programs. Moreover, some employers are creating new programs, issuing directives, and training managers and employees on new violence prevention issues; such programs are viewed as helping to ensure worker health and productivity, and in minimizing potential liability. Finally, some employers, if they have not already done so, are setting up disaster preparedness committees charged with establishing appropriate policies. Numerous entities have drafted disaster protocols and shared them as appropriate with employees; the Federal Emergency Management Agency (FEMA) has issued a step-by-step guide on how to create and maintain a comprehensive emergency management program. The guide is designed for use by manufacturers, corporate offices, retailers, utilities, or any organization with a sizable number of employees.[60]

In light of recent natural disasters, specifically Hurricane Katrina, workplace security has taken on additional urgency. Water sector facilities are encouraged to carefully consider what measures their respective states have implemented with regard to emergency services following 9/11 and Katrina.[61] The Water SSP contains a compendium of information that is useful to the water sector in establishing such emergency response programs.

Employers who have reason to suspect the presence of a dangerous pathogen, and fail to take reasonable protective measures, could be held liable for resulting damage to employees under the various common law negligence theories addressed above in Section II. As one example, water sector facilities in areas where anthrax has been discovered may wish to emulate those employers in the Washington, D.C. area who deployed indoor environmental specialists to test mailrooms following information that anthrax-laced letters delivered through the Brentwood Central Post Office in Washington, D.C. in 2003 had the potential to spread anthrax to other mail that came in contact with letters delivered to U.S. Senators.

The London Tube attacks of July 2005 resulted in explosions in three Tube stations and on a double-decker bus killing 52 people. This event coupled with another failed bombing attempt in London two weeks later, and other worldwide instances of similar terrorist's threats have cumulatively heightened the awareness of any employer's obligation to be cognizant of the working environment they are maintaining for their employees. This new class of threats that highlighted the vulnerability of the underground transportation system in London presents many lessons learned for protecting the network of underground water distribution or collection infrastructure owned and operated by facilities in the United States.[62]

C. Employer Response to Potential Health Impacts to Employees from Terrorist Acts or Threats of Terrorism

1. Overview

In addition to causing deaths, acts of terrorism or vandalism often leave survivors with debilitating physical or emotional injuries; their families and other individuals may also suffer physical or emotional trauma. Injuries sustained by employees while on the job could trigger the application of worker's compensation benefits under state law.[63] Individuals injured or traumatized by a terrorist attack may request a workplace accommodation for a disability. Some employees may seek leave to recover from an injury, to engage in rehabilitation, or to assist other family members in doing so. Therefore, employers faced with acts of terrorism or other serious workplace disruptions should be aware of leave requirements under federal, state and local laws, as well as the entities' own internal policies governing leave.

2. Employee Disabilities and Employer Accommodations Including Leave

Employees may be disabled as a result of a terrorist incident and entitled to relief under federal law. As noted herein, leave might be a "reasonable accommodation" in some circumstances under the *Americans with Disabilities Act* (ADA). An employer need not provide paid leave beyond that which is provided to similarly situated employees who do not take leave. As a general rule, an employee with a disability who is granted leave as a reasonable accommodation is entitled to return to his or her same position unless the employer demonstrates that holding open the position would impose an "undue hardship," a significant hurdle. According to the Equal Employment Opportunity Commission (EEOC), if an employer cannot hold a position open during the entire leave period without incurring undue hardship, it must consider whether it has a vacant, equivalent position for which the employee is qualified and to which the employee can be reassigned.

Recent press accounts and studies have documented increased incidents of such conditions as Post-Traumatic Stress Disorder since the events of 9/11. Individuals with such injuries often request leave from work, and employers must respond to such requests in accordance with the ADA, 42 U.S.C. § 12112, et seq.[64] and the *Family and Medical Leave Act of 1993* (FMLA), 29 U.S.C.A. § 2601. Employers should note that common law has limited an individual's ability to claim a disability under the ADA, requiring that the claim should be assessed with respect to any mitigating or corrective measures employed. See *Murphy v. United Parcel Service, Inc.* 527 U.S. 516, (U.S. 1999).[65]

The employment discrimination provisions of the ADA prohibit employers with 15 or more employees from discriminating against "qualified individuals with disabilities" in regard to all terms of employment, and it requires employers to make "reasonable accommodations" for known disabilities. An individual has a "disability" if he or she has a significant physical or mental impairment that substantially limits a major life activity. He or she is "qualified" under the Act if the essential functions of the position can be performed with reasonable accommodation of the disability. Whether an individual is protected by the Act is always handled on a case-by-case basis. The federal FMLA, on the other hand, requires employers of 50 or more employees to give eligible

employees (based on service records) an unpaid leave from a job for family or serious medical reasons. There is a cap on how much leave an employee can take.

In light of the foregoing, employers should take seriously leave requests (or other accommodation requests) triggered by terrorism or vandalism, particularly because such leave is mandated by the FMLA for certain serious conditions and has been determined by the EEOC and various courts to be a "reasonable accommodation" under the ADA. Water sector facilities owners and operators may want to consider designating a single official who is properly trained in the requirements of the laws to receive and handle such leave requests in a prompt, fair, and consistent manner.

3. Voluntary and Mandatory Medical Monitoring

Recently, some employers have requested, not demanded, that employees subject themselves to health monitoring. This issue may arise, for example, if an owner or operator believes that a pathogen may be present in the workplace or that a release of a hazardous substance may have occurred as a result of an accident, an act of vandalism, or an act of terrorism.

Medical examinations and inquiries as part of a voluntary medical program are lawful under federal law. As a general matter, however, medical information gathered in a voluntary medical program must be kept confidential in a separate employer file. Sharing such information with appropriate law enforcement or medical authorities in exigent circumstances might be lawful, particularly if the employee provides written consent to do so.

The issue of mandatory monitoring of employee health has not been heavily discussed; however, municipal employers should approach any mandatory monitoring very cautiously. Under the *Americans with Disabilities Act*, it is unlawful, with few exceptions, for an employer to require a medical examination of an employee or to make inquiries as to employees' health conditions. Medical examinations or inquiries of employees are permitted only when they are job-related and consistent with business necessity; information gathered must be kept by the employer in a separate confidential file. Such a practice would come under exacting scrutiny, and the employer would bear the burden of proving business necessity. Both employers and employees should be mindful that the court will look closely for a distinction between a discriminatory act that warrants legal relief and a workplace dispute. See *Conrad v. Board of Johnson County Com'rs*, 237 F.Supp.2d 1204 (D. Kan. 2002). Again, municipal employers should consult state and local law, as well as collective bargaining agreements, for additional guidance on this issue.

These same laws generally do not require an employer to retain an employee with unwarranted fears of coming back to work. However, before discharging an employee who appears to have an unwarranted fear of the workplace, the employer should consider the requirements of the ADA and worker compensation laws, as well as possible adverse morale issues for remaining employees, before doing so. In addition, the employer should consult other state laws and regulations, including any state FMLA laws that may exist.

4. Accommodation of Employees' Military Service

The *Federal Uniformed Services Employment and Reemployment Rights Act* (USERRA) protects the rights and benefits of employees who are in the military and/or who report for military services. 38 U.S.C.A. § 4301, et seq. Some state laws provide more generous benefits; employers should check the laws in each state where they have employees. Some municipal ordinances also specifically address military leave.

As a general matter, employers (including states and municipalities) must provide an unpaid leave of absence for employees to serve in the uniformed services. In addition, the USERRA protects employees' benefits and rights during and upon return from military leave by: prohibiting discrimination and retaliation; allowing use of paid time off held by the employee; guaranteeing continued health insurance coverage while on leave; generally guaranteeing reemployment upon return from leave; preserving seniority and pension benefits when re-employed; prohibiting discharge without cause for specific periods of time after return from service; and providing an enforcement mechanism and remedies, including damages, attorneys fees and costs, if the Act is violated.

With respect to the FMLA, the federal statute requires that upon return from leave the employee be restored to the position he or she held at the start of leave or to an equivalent position with equivalent employment benefits, pay, and other terms and conditions of employment. There is an exception to this job restoration requirement for certain highly compensated employees. As noted above, USERRA generally requires reemployment upon return from leave. The ADA, FMLA and USERRA each require the preservation of certain employee benefits (including health insurance coverage) during leave.

CHAPTER ENDNOTES

56 The regulations further provide a list of factors to be considered when determining whether a particular entity meets the test of "political subdivision." Id. at § 1975.5(c). The regulations also give examples of entities that are normally considered exempt from the provisions of OSHA as a political subdivision of a State, including "State, county and municipal law enforcement agencies . . . State, county and municipal judicial bodies; . . . [and] State, county and municipal public school boards and commissions." 29 C.F.R. § 1975.5(e). Additionally, the regulations provide examples of entities that "probably" are exempt from OSHA, including "harbor districts, irrigation districts, port authorities . . .; {and] municipal transit entities. . ." Id. Finally, the regulations also indicate that certain entities "would not normally" be regarded as a political subdivision of a State, and would therefore not be exempt from the Act: "[p]ublic utility companies. . ." Id.

57 Available on OSHA's web site, www.osha.gov, this guidance may prove useful.

58 For a detailed review of negligence standard applied to threats of terrorist attacks, see generally section II. B. *supra*.

59 See note 26 supra for a discussion of the per se negligence standard.

60 A copy of the FEMA guide is available at http://www.nmhc.org/Content/ServeFile.cfm?FileID=2673.

61 See, e.g., California Governor's Office of Emergency Services programs. The California Governor's Office of Emergency Services website is available at: http://www.oes.ca.gov. See also, Indiana Department of Homeland Security programs. Indiana Department of Homeland Security website available at: http://www.in.gov/dhs/.

62 The U.S. Department of Homeland Security (DHS) Joint Information Bulletin on implications for homeland security of the London train bombings is available to WaterISAC subscribers on the secure portal. For more information on the WaterISAC, see Section IV (E), *infra*.

63 Much of the following discussion of employee's rights was adapted from the original copyrighted *Checklist*.

64 This legislation has received some negative treatment, See *Hamilton v. Rheem Mfg. Co.* 158 F.Supp.2d 931, 933 (W.D.Ark. 2000). "The ADA prohibits covered employers from discriminating against individuals on the basis of their disabilities". See 42 U.S.C. § 12112(a). Specifically, it prohibits an employer from discriminating "against a qualified individual with a disability because of the disability of such individual in regard to job application procedures, the hiring, advancement, or discharge of employees, employee compensation, job training, and other terms, conditions, and privileges of employment." 42 U.S.C. § 12112(a). Although the statute is broadly worded and appears to be all-inclusive, two recent Supreme Court cases have substantially limited its application. See *Murphy v. United Parcel Serv., Inc.,* 527 U.S. 516, 119 S.Ct. 2133, 144 L.Ed.2d 484 (1999) and *Sutton v. United Air Lines, Inc.*, 527 U.S. 471, 119 S.Ct. 2139, 144 L.Ed.2d 450 (1999).

65 This case has received negative treatment but is not overruled; some jurisdictions have decided not to extend the full holding.

Chapter 4

Managing Information with the Potential to Impact the Security of Water Sector Infrastructure

Managing Information with the Potential to Impact the Security of Water Sector Infrastructure

A. The Delicate Balance between the Need to Keep Information from Terrorists and the Government's and Public's Right to Know

Information about a facility, its engineered structures, and how the facility is managed, is the lynchpin to developing and maintaining a secure facility. Legal mandates governing water sector information ideally strike the appropriate balance of competing public interests by allowing dissemination of sufficient information to the appropriate government officials, and to the public, to allow them to weigh the risks of various facilities in a community, and to meaningfully participate in local governmental emergency preparedness programs—while at the same time keeping sensitive security information out of the hands of terrorists. This is no small or easy task.

Information plays a critical role in all aspects of infrastructure security, from physical plant security, to screening and hiring of reliable workers, to the development and implementation of effective emergency preparedness plans. Sharing security information with organizations and individuals with a "need to know" is essential not only to facilitate emergency preparedness planning, but also to design effective action by facility operators and "first responders" such as the police, hospitals, and fire departments in the event of an actual attack. Nevertheless, that same critical security information in the hands of a terrorist can be used as a devastating "blueprint" for attack.

Four groups, each with different needs and concerns, can be expected to have somewhat different approaches to infrastructure security information, according to the National Academies of Science: (1) the DHS and agencies with responsibility for national security; (2) water sector industries; (3) federal, state, and local agencies involved with preparedness, emergency response, and environmental regulation; and (4) the general public.[66] Federal agencies responsible for homeland security can be expected to favor restrictions on information sharing to minimize potential risks. Water sector facility owners and state and local agencies need readily available information and tools that can be implemented practically and routinely, although the needs vary widely from facility to facility, and one jurisdiction to another, depending upon the size of the population served, the location of water sector facilities in relation to other industry, and so on.[67] The public needs enough information to maintain confidence in the safety of the water supply and treatment systems. The public also wants access to the means to protect itself in the event of an attack, and the ability to determine when the systems are again safe and reliable following attack.[68] Somehow these diverse approaches must be balanced by the legal system which controls access to security related information.[69] The Water SSP details methods for collecting and protecting vulnerability assessments and other sensitive information, while at the same time securely sharing that same information with government entities and first responders who have a "need to know."[70]

Even facilities with adequate physical security measures, such as access controls, fences, and monitors, are vulnerable to terrorist attack if detailed information about those systems falls into the wrong hands. Because there is no more critical security issue than the control and management of sensitive infrastructure information which details system vulnerabilities and necessary corrective measures, consideration of legal restrictions on access to security documentation begins with those documents.

B. Preventing the Unauthorized Disclosure of Water Infrastructure Security Information that Would Directly Aid Terrorists

1. The Evolution of Statutory Protection for Vulnerability Assessments

a. Access to Vulnerability Assessments Prepared by Water Suppliers

The Bioterrorism Act anticipated the need to protect CWS vulnerability assessments from disclosure. The Act specifically exempts such vulnerability assessments from disclosure under the *Freedom of Information Act*.[71] EPA is obligated to protect the information contained within the assessments from disclosure, and has developed an information protocol that strictly limits access to these assessments even within the EPA.[72] Although not yet tested in court, the federal law appears to preempt any contrary state law or local ordinance that would require a CWS covered by *The Bioterrorism Act* to disclose the vulnerability assessment to entities other than governmental agencies with a need to know. Water supply vulnerability assessments were required to be submitted to the federal government (EPA) for review.

Since 9/11, the federal government has been grappling with the disclosure of vulnerability assessments and other sensitive information, most notably in the context of critical energy infrastructure information (CEII). Even before that, the *Freedom of Information Act* protected against disclosure by federal agencies of national security information, as well as any other information that was required to be kept confidential pursuant to federal statute. 5 U.S.C.§ 552 (exemptions 1 and 3).

Early on, the Supreme Court upheld the Navy's refusal to release nuclear information that could compromise national security during an environmental assessment pursuant to the *National Environmental Policy Act* (NEPA) in *Weinberger v. Catholic Action of Hawaii*, 454 U.S. 141, 143 (1984). The Supreme Court noted that Congress wrote NEPA in a manner which reconciled its disclosure requirements with the need of national security and Freedom of Information disclosure requirements. NEPA expressly makes disclosure of the contents of an Environmental Assessment or Environmental Impact Statement (EIS) subject to the provisions of the *Freedom of Information Act*. 42 U.S.C.§ 4332(C)("copies of such statement... shall be made available to the President, the Council on Environmental Quality, and the public as provided by section 552 of Title 5"...). The Supreme Court, in construing the requirements of NEPA and FOIA, held the following:

> **FOIA was intended by Congress to balance the public's need for access to official information with the Government's need for confidentiality.... Thus, [NEPA] §102(2)(C) contemplates that in a given situation a federal agency might have to include environmental considerations in its decision making process, yet withhold public disclosure of any NEPA documents, in whole or in part, under the authority of an FOIA exemption. 454 U.S. at 143-44.**

The Federal Energy Regulatory Commission (FERC) recently achieved just such a balance in promulgating its regulations concerning the disclosure of CEII information contained in materials submitted to FERC by the energy industry. 18 CFR Parts 375 and 388; FERC Order 630,102 FERC 1161,190 (Feb 21, 2003) as amended by FERC Order 630-A, 104 FERC 61,106

(July 23, 2003). The definition of CEII includes only information that could aid terrorists and is exempt from disclosure under FOIA. See 18 CFR §388.113(c)(ii)-(iii) (2004). All safety information not exempt from disclosure under FOIA or other federal law is made available to the public. *The Bioterrorism Act* and SDWA amendments establish a disclosure system for CWS that is nearly identical to that established for CEII.

b. Access to Vulnerability Assessments Prepared by Wastewater Treatment Facilities

The statutory requirements that protect water supply vulnerability assessments from unauthorized disclosure are ahead of federal legislative efforts to protect similar assessments performed by wastewater treatment. The Department of Homeland Security, pursuant to Section 550 of its *Appropriations Act of 2007*, is authorized to collect sensitive but unclassified (SBU) information regarding chemical-terrorism vulnerability that would have covered aspects of wastewater sector chemical disinfectant processes, including storage and use of chlorine. However, such facilities were specifically exempted by the interim final regulation.[73]

Federal regulations, found at 6 CFR Part 27.400, authorize the Department of Homeland Security to apply the protective marking, "Chemical-Terrorism Vulnerability Information (CVI)", to such information and alert the recipient that it is exempt from public disclosure and is afforded other safeguarding protections. The marking also informs the person in possession of CVI that it must be handled according to specific procedures.

i. State Statutory Protections Under Freedom of Information Laws

Many CWSs and POTWs , however, are covered by state-enacted equivalents of the *Freedom of Information Act* and the *National Environmental Policy Act*.

For example, information in the possession of municipal water suppliers or wastewater treatment agencies is generally subject to disclosure requirements, pursuant to requests from the public, unless the information qualifies for specific statutory exemptions. Some states have acted after 9/11 to explicitly exempt security information, including vulnerability assessments, that would aid terrorists. For example, California exempts disclosure of a "document prepared by or for a state or local agency that assesses its vulnerability to terrorist attack or other criminal acts intended to disrupt the public agency's operations and that is for distribution or consideration in a closed session." Cal. Gov't Code § 6254 (aa). Georgia's statute prevents release of "records, the disclosure of which would compromise security against sabotage or criminal or terrorist acts and the nondisclosure of which is necessary for the protection of life, safety, or public property, which shall be limited to the following: (i) Security plans and vulnerability assessments for any public utility, technology infrastructure, building, facility, function, or activity in effect at the time of the request for disclosure or pertaining to a plan or assessment in effect at such time." Ga. Code Ann. § 50-18-72.15(A)(2006).

Many other state freedom of information statutes contain general exemptions that would probably operate to protect vulnerability assessments from public disclosure. For example, in New York, there is an exemption to disclosure for information that, if disclosed, "could

endanger the life or safety of any person." NY Pub. Off. § 87(2)(f); See also Conn. Gen. St. § 1-210(b)(19) (exempting disclosure when there are "reasonable grounds to believe disclosure may result in a safety risk..."). In Colorado, documents may be withheld if a district court agrees with the document's custodian that disclosure could "do substantial injury to the public interest." Colorado Rev. Statutes 24-72-204 at 6(a). Therefore, it is important as a preliminary matter to check the requirements of the applicable state freedom of information law.

ii. Other State Statutory and Common Protections

In general, legally privileged information is exempt from disclosure under state law. The issue of privilege most frequently arises when information is sought by a litigant. This issue has arisen in the cases where plaintiffs, through discovery, sought access to information from a facility or its owner following the 9/11 attacks, an eco-terrorism attack, or acts of vandalism. In such situations, depending on the specific circumstances, the state's privilege doctrines may afford protection for vulnerability assessments from disclosure. However, the privilege also may be applicable to other work product, if, for instance, counsel hires a consultant to evaluate the potential vulnerability of a system for purposes of obtaining insurance or for assessing the potential fiscal status of the system.

In the late 1990s, about a half dozen jurisdictions adopted self-evaluative privileges to promote the public policy goal of encouraging entities to voluntarily undertake environmental audits. For instance, Colorado's law includes three provisions which, taken together, comprise an environmental self-audit privilege. C.R.S. sections 13-25-126.5 (audit privilege for documents arising from environmental self-evaluation); 13-90-107(1)(j) (testimonial privilege for voluntary self-evaluations); and 25-1-114.5 (penalty immunity for voluntary disclosures arising from self-evaluation). Generally, the audit privilege protects against disclosure of an audit in civil or criminal discovery (including administrative actions) unless the privilege is waived or there is a determination by an administrative law judge that the entity claiming the privilege was or is in noncompliance and did not or will not take appropriate action to achieve compliance within a reasonable time period. The privilege does not apply to information and data required by law to be available to the state, and it does not prevent public release of "non-privileged information" (such as the fact that a violation occurred and facts underlying the violation).

Even in the absence of statutory protections that prevent dissemination of vulnerability assessments to entities other than governmental agencies, POTWs and other wastewater treatment owners and operators may be able to withhold such information based on common law principles. Courts have applied common law self-audit privileges in the environmental context, but not uniformly. See, *e.g.*, *Reichhold Chemical v. Textron*, 157 F.R.D. 522, 527 (N. D. Fla. 1994) (landowner in CERCLA case entitled to qualified privilege for retrospective analysis); *Joiner v. Hercules, Inc.*, 169 F.R.D. 695, 698-99 (S.D. Ga 1996) (self-audits of compliance with environmental laws are protected under the self-critical analysis privilege). Cf. *Louisiana Environmental Action Network, Inc. v. Evans Industries, Inc.*, No. 95-3002, 1996 U.S. Dist. LEXIS 8117, at *7-8 (E.D. La. June 10, 1996) (voluntary environmental self-analyses are

"not protected by a privilege of self-critical analysis" because the "possibility of disclosure during discovery" would not deter such evaluations); *U.S. v. Dexter*, 132 F.R.D. 8, 10 (D. Conn. 1990) ("in an action brought by the United States government to enforce the Clean Water Act ... a corporation does not have a qualified privilege against disclosure of self-evaluative documents."); *Carr v. El Dorado Chemical Co.*, No. 96-1081, 1997 U.S. Dist. LEXIS 5752, at *23-25 (W.D. Arizona, Apr. 14, 1997) (self-critical analysis privilege improper because disclosure would not discourage defendant from conducting future audits).

C. Required Disclosure of Vulnerability Assessments to the Government

While *The Bioterrorism Act* now requires the submittal of CWS vulnerability assessment to EPA, there is no equivalent federal law requiring submittal of voluntary vulnerability assessments by wastewater facilities; nor are there federal disclosure requirements analogous to those covering Risk Management Plans prepared by regulated entities under Section 112(r) of the *Clean Air Act*. 42 U.S.C. § 7412(r) (2001). Generally, any vulnerability assessment that a municipal or private wastewater facility decides to undertake on a purely voluntary basis—in addition to, and separate from, any assessment or report required by law—is not likely by itself to require disclosure to the federal government. However, state laws and the specific relationship between a municipal wastewater authority and other branches of the local government including city councils and a Mayor's office may require such information exchange. See, e.g., City Code of Stamford, CT, Ch. 52, Art. II, § 52.6 (suggesting that legislative bodies of the City of Stamford, the Board of Representatives and the Board of Finance have authority to examine "all records, data and property" of any department, employee or other member of municipal government). Further, disclosure may be required if local, state or federal enforcement authorities later target such assessments with an information request or in legal discovery. In narrow instances, privilege doctrines may be available to protect the vulnerability assessment from disclosure to an agency or department.

As noted below, some states have created statutory or regulatory audit privileges that may protect voluntary risk assessments from disclosure requirements. In addition, some states have recognized a common law self-evaluative privilege. Although many courts (including the federal courts) have refused to apply a self-evaluative privilege in the context of government investigations/enforcement, the specific law in each state should be consulted. Finally, government disclosure of vulnerability assessments provided by a municipal wastewater treatment agency to a state or municipal entity may be eligible for confidentiality from further disclosure under state and/or local "sunshine" laws or freedom of information acts.

The federal government would likely be able to obtain a voluntary vulnerability assessment if the assessment is the subject of an enforcement agency's information request, especially if it is not prepared at the request of an attorney. There is no federal audit privilege that can protect such assessments if such a request is made. However, an exception to the disclosure requirement may apply if the vulnerability assessment qualifies for protection under the attorney-client privilege. Generally, however, the attorney-client privilege applies to information communicated in a confidential way by a client to a lawyer for the purpose of securing legal advice. If the primary purpose of a vulnerability assessment is to facilitate communication with a lawyer regarding legal issues, the assessment may be privileged and not subject to federal disclosure requirements. Even if the privilege applies, however, the factual information within the

assessment may not be protected if it can be obtained from other sources. The attorney work-product privilege also could apply to vulnerability assessments that were conducted at the request of an attorney in anticipation of litigation or in preparation for trial.

In a government enforcement action, citizen suit, or in private litigation, persons may seek to obtain a copy of a vulnerability assessment. With respect to an information request from a federal agency, such as EPA seeking information pursuant to Section 114 of the *Clean Air Act*, no privilege would apply. In private litigation, assuming relevance, disclosure would be required if the assessment is not privileged unless the municipal wastewater treatment agency is able to obtain a protective order from the court.

D. Access to Water Sector Facilities Designs, Plans, and Specifications

Avoiding disclosure of water sector vulnerability studies is only one step, an obvious one, in preventing sensitive information from reaching the hands of would be terrorists. Many facilities owners and operators also decry the fact that basic plant design and system information is sometimes readily available to the public. As just analyzed, state and local freedom of information laws and ordinances vary widely in what information must be disclosed by publicly-owned water sector facilities. In the aftermath of 9/11, federal dam design information was withdrawn from the Internet and government reading rooms, and is now subject to disclosure restrictions as critical energy infrastructure information (CEII); those restrictions were outlined previously. Water sector utilities often face difficult choices when it comes to protecting sensitive design information, especially if the utility is trying to solicit bids for new construction or expansion projects of their plants and/or collection systems. This dilemma in turn has led many water sector utilities to question if there are ways to keep sensitive plant design and blueprints from public disclosure.

As a first step in answering this question, it is important to note that some state laws that prevent disclosure of vulnerability assessments would also cover plant designs and system specifications. Many state freedom of information statutes contain general exemptions that would probably operate to prevent disclosure of plans, designs and specifications[74] from public disclosure, as previously detailed.

One current area of potential federal protection for design information that water utilities should be aware of is the Protected Critical Infrastructure Information (PCII) Program, run by DHS. This program is designed to facilitate information sharing between the federal government and key industries by ensuring that sensitive security-related information shared by industry with the federal government is protected from public disclosure. The program was created by the *Critical Infrastructure Information Act* of 2002 (CII) and is being implemented by DHS under a Final Rule published on September 1, 2006.[75] If security-related information meeting the requirements of the CII is shared with the federal government, that information will then be protected from public disclosure under the *Freedom of Information Act*, state and local disclosure laws, and from use in civil litigation. By creating such protections, the program hopes to encourage industry and utilities to share security-related infrastructure information with the federal government. It should be noted however that this is only a federal program, and does not cover information shared with local or state governments.[76] Although there is no targeted federal protection yet for water sector facility designs that directly addresses this problem, many experts believe that DHS and federal lawmakers will soon have to draft legislation that makes the difficult balance in this area between disclosure and secrecy.

E. Facilitating the Dissemination of Security Information and Assistance to Thwart Terrorism

Ironically, the same security information that would aid terrorists is essential to prevent attacks or to effectively respond when incidents occur. Owners and operators of water sector infrastructure generally make facility security information available to those individuals in their own workforce, as well as local, state and federal agencies that act when a threat or an actual attack occurs. The problems inherent with security information sharing are among the most difficult that water sector facilities and the EPA face.

In 1998, EPA was designated the lead federal agency to coordinate water security efforts in the water sector, which had been identified as one of the eight most critical U.S. infrastructures. At that time, drinking water and wastewater utilities were concerned mainly with "home-grown" threats, such as vandalism and damage to cyber systems and infrastructure by pranksters and disgruntled employees, and by accidents. After the terrorist attacks of 9/11, security efforts intensified and changed course. EPA and water utilities broadened their view of potential security threats to include deliberate contamination of water by bacterial, chemical, and radiological substances, as well as cyber terrorism and intentional destruction of infrastructure.

A key tool for the water sector in disseminating security information is the Water Information Sharing and Analysis Center (WaterISAC). WaterISAC was established by Presidential Decision Directive 63, which mandated the establishment of ISACs for various components of the nation's infrastructure and called for the sharing of security and sensitive information among elements of the government and private sectors. WaterISAC is a subscription-based service open to all drinking water and wastewater utilities within the United States, regardless of the size of the population served or the public or private status of the ownership of the facility. In addition to the water resources facilities, state administrators as well as certain EPA personnel also have access to the information. Many organizations within the water sector participate in WaterISAC and are able to share the latest research on possible threats and information that facilitates effective emergency response in the event of attack. WaterISAC plays an important role in disseminating sensitive risk and incident information to members of the water sector and is the primary mechanism for effectively and efficiently sharing security-related information within the water sector. It allows utilities within the water sector to share incident information in a standardized format. Additionally, EPA also obtains input into research and technical support products through the WaterISAC; sensitive security research findings are posted on the secure WaterISAC portal and subscribers are asked to review and comment using the secure bulletin board. Comments are then forwarded to EPA for consideration.

The Water Sector Coordinating Council (WSCC), a group representing the water sector that was organized to give advice to DHS, has recognized WaterISAC, including its supplementary WaterSC, as the primary communication tool within the water sector. The recently issued Water SSP, endorsed by the WSCC and the Water Sector Government Coordinating Council (GCC), notes that the WaterISAC also plays an important role in communication of critical water sector information between utilities and federal agencies such as EPA, DHS, and the FBI. These communications are used to share intelligence and threat warnings related to physical and cyber attacks, and well as contamination. Federal agencies regularly prepare and update threat information affecting drinking water and wastewater utilities, and this information can be shared through the WaterISAC. Additionally, water sector utilities can use the WaterISAC to coordinate security activities with local FBI offices.[78]

The National Research Council (NRC) of the National Academies of Science estimates that WaterISAC currently reaches over a thousand individuals at more than 500 water utilities that provide water services to 65 percent of the American population.[79] A "Water Security Channel" (WaterSC) is managed by WaterISAC and is designed to reach even the drinking water and wastewater utilities that have not subscribed to the more comprehensive services of the WaterISAC. NRC further estimates that WaterSC reaches 12,122 individuals at 10,721 organizations.[80] WaterSC affiliates include utilities as well as state organizations with *Clean Water Act* primacy, other government organizations, engineering firms, and researchers. The services of WaterSC are free and available to all utilities and organizations concerned with water security. Both WaterISAC and WaterSC are partially funded through an EPA grant.

WaterISAC and WaterSC security protocols require users to be authenticated before accepting and authorizing access to information. Because WaterISAC handles highly sensitive information, its vetting process is more rigorous. WaterISAC also has a double authentication protocol in place to ensure that only authorized individuals access a designated document. When new and urgent information becomes available, WaterISAC and WaterSC subscribers are informed via e-mail and online notification databases. Subscribers can also be notified by text messages directly to their cell phones. The message would provide the location of the information including a link to its contents and a brief overview so that the subscriber can determine if the document would be of use in the particular circumstance. Additionally, WaterISAC and WaterSC Web sites host newly released information in file format.

An additional communication software platform exists in the Homeland Security Information Network (HSIN), which was launched by DHS as a communications tool to make federal information available to a broad range of U.S. businesses and individuals. HSIN is being offered to all critical infrastructure sectors, including the water sector. Because of the vast audience, sensitive data cannot be made available on HSIN, as it can be on WaterISAC. After an evaluation of the HSIN's capabilities, a recommendation to integrate HSIN into the suite of communication tools used by WaterISAC was made and approved by both the WaterISAC Board and the WSCC. HSIN, as well as WaterSC, will be available at no cost to all utilities, state primacy organizations, government organizations, engineering firms, researchers, and other interested parties.

Another key tool available to water sector utilities when engaging in security planning and studying how to disseminate security-related information is the recently released Water SSP.[81] As analyzed previously, the Water SSP was released in May 2007 and is part of DHS's National Infrastructure Protection Plan (NIPP) and is intended to establish a coordinated response to national priorities, goals, and requirements for critical water sector infrastructure. It provides a critical component of the federal government's efforts to enhance protection of the nation's water sector infrastructure and communicate security information to water utilities.

The Water SSP was developed through a national collaborative effort, with significant input from both the WSCC and the GCC. It includes a variety of important security information for the water sector, including:

- **an overview of the water sector;**
- **a description of ongoing efforts by the federal government and water sector security partners to identify, prioritize, and coordinate key sector resources that could, if compromised, result in economic or public health impacts;**

- **a description of appropriate risk assessment procedures for the water sector;**
- **development of a water sector process for risk-based prioritization of assets;**
- **discussion of how the water sector develops and implements protective programs that can be used throughout the sector; and**
- **discussion of on-going security-related research and development initiatives by EPA and DHS that affect the water sector.**

The Water SSP is the most comprehensive document published by the federal government dealing with water sector security post-9/11, and serves as an important reference for water sector utilities to consult when engaging in security planning.

Other sources of communication and assistance for security-related issues available to water sector utilities are Water and Wastewater Agency Response Networks (WARNs) and the Emergency Management Assistance Compact (EMAC). WARNs are networks of utilities that have agreed to help other utilities respond to, and recover from, various types of emergencies. The purpose of a WARN is to provide rapid deployment of emergency services and personnel to a water sector utility that needs immediate assistance in resuming normal operations after an unexpected disruption. These networks are often formed within states, and are made up of utilities from a state that have all signed a Mutual Aid and Assistance Agreement to come to the aid of other intrastate utilities in the event of an accident, natural disaster, or terrorist attack. The aid provided can be in the form of personnel, materials, equipment, or other necessary resources to restore operations of a water or wastewater system. These networks are usually voluntary in nature and there is no cost to join.

The EMAC, in comparison, is an interstate compact between all 50 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands that provides form and structure to interstate mutual aid. Through EMAC, a disaster impacted state can request and receive assistance, including water sector assistance, from other member states. The EMAC is administered by the National Emergency Management Agency (NEMA) and has been authorized by Congress.[82]

Notwithstanding all of these available methods for disseminating information to the water sector, a report of the National Research Council of National Academy of Sciences found that vital information on priority contaminants and threats that could improve utilities' response capabilities has been classified and cannot be shared with other utilities, even through secure dissemination mechanisms. The National Research Council report was a review of EPA's progress in developing permanent water security research and technical assistance plans. According to the NRC report, EPA should find ways to make sensitive information on water security available to parties that need it, including drinking water and wastewater utilities. In addition to utilities, parties with a potential need to know include state and local governments, emergency responders, and the public.

To improve communication of its research, EPA should obtain early input and involvement from parties that most need security information, according to the NRC. In its view, communication strategies are more likely to be effective if target audiences are asked for input before efforts are made to communicate information. Current web-based approaches to dissemination should be improved because "the number

of anticipated research products will undoubtedly make it difficult for utilities to keep up with the information," the NRC report concluded.

In the meantime, EPA should continue to use the computer-based WaterISAC to alert stakeholders to the availability of sensitive materials. EPA also should consider developing a web-based information portal to make the research findings "easily and readily available to the full range of stakeholders," the NRC report stated. The agency should develop feedback mechanisms to learn what products have been useful and what improvements may be needed, according to the report.

The aforementioned Water SSP effectively addressed many of these criticisms. There are also concrete examples of water sector utilities effectively sharing information during a time of crisis. An excellent example of such cooperative use of sensitive water security information occurred in June of 2006. The Philadelphia Water Department (PWD) was contacted by the Pennsylvania Department of Environmental Protection (PADEP) regarding an unusual fish kill in a creek upstream of the City of Philadelphia (City). This alert was the result of an early warning system designed, built, and operated by PWD to quickly convey water quality issues from upstream users to downstream users. The fish kill had been detected that afternoon at the outfall of a suburban sewage treatment plant. The Wissahickon Creek is a major tributary to the Schuylkill River which is a source of City drinking water. Initial speculation about the cause of the fish kill included a possible natural occurrence, accidental discharge, or terrorism.

Within a day, the fish kill had spread about a half mile downstream. PWD deployed field crews to the Wissahickon Creek to make observations, conduct flow measurements for travel time estimates, and take water samples. PADEP immediately informed PWD that some form of cyanide may have been involved and that the EPA and FBI were investigating the situation. City management convened a meeting of PWD, PADEP, the Police Department, the Health Department, the Law Department, the Park Commission, the Mayor's Press Office, and the Office of Emergency Management. Lacking concrete information on the contaminant source, the type or duration of the discharge, and the potential health and water treatment risk, the City issued a public health advisory prohibiting use of the Wissahickon Creek and Schuylkill River and temporarily closed its drinking water intakes on the Schuylkill River.

The following day, additional investigation and testing indicated that the event was localized upstream and there was no danger to the City or its drinking water. Restrictions on the Creek and River were lifted and the drinking water intakes were reopened. A week later, an upstream vaccine research facility notified EPA that there had been an accidental release of about 25 gallons of potassium thiocyanate, a substance commonly used in making antibiotics, into the sewer system. Apparently, the chemical combined with chlorine used for disinfection at the suburban sewage treatment plant and temporarily made the plant's effluent toxic to fish due to increased cyanide concentrations. The vaccine company and the incident are still under investigation by state and federal authorities. Nevertheless, PWD's early warning system and PWD's ability to quickly respond to a potential crisis are examples of effective response action based on early sharing of information.

F. Obtaining Sensitive Employee Information to Prevent Acts of Terrorism: Interview Questions, Background Checks, Information Gathering, and General Monitoring of Employees

Examples of personnel procedures that may enhance security at a facility include applicant background checks and employee screenings, barriers to facility access without appropriate credentials, worker/visitor surveillance, management of employees who arouse suspicion, effective responses to possible workplace violence, and cooperation with governmental authorities in anti-terrorism investigations and counter-measures. As water sector employers decide whether to implement new or improved security measures relative to their workers and employees, legal issues regarding employees' civil rights and privacy, or contractual issues involving union-negotiated agreements, may be raised.

Employers routinely require applicants to provide certain types of personal information as part of the hiring process. Employers can confirm and supplement that information through various methods, including references, background investigations, credit checks, medical screening, and drug testing. With the expansion of the Internet, employers' information collection methods are becoming increasingly sophisticated. With that expansion of capability comes a heightened concern that these enhanced data gathering and monitoring methods will invade employees' privacy or violate civil rights.

1. Employee Civil Rights Protections

Since 9/11, one of the most pressing employment law questions facing water sector employers is what type of screening of employees and job applicants is lawful and prudent. Despite the potential legal hurdles, new procedures are likely to provide enhanced protection of both employees and the general population. There is a wide variety of state and federal laws prohibiting different types of employee screening measures, many but not all of which are applicable to municipal employees. Screening measures cannot be used to discriminate on the basis of race, color, age, religion, national origin and sex.[83] 42 U.S.C. § 2000e et seq. (Title VII of the *Civil Rights Act* hereinafter "Title VII").

Title VII is directly relevant to employers contemplating deterrence of acts of terrorism by means of screening out employees based on national origin or religion. For example, employer profiling of employees or applicants, including those individuals with origins in Arab countries or belonging to the Muslim faith, violates equal protection principles and Title VII. Shortly after the events of September 11, the Chair of the U.S. Equal Employment Opportunity Commission (EEOC) called on all employers and employees across the country to promote tolerance and guard against unlawful workplace discrimination based on national origin or religion. The EEOC encouraged employers to: reiterate policies against harassment based on religion, ethnicity, and national origin; communicate procedures for addressing workplace discrimination and harassment; urge employees to report any such improper conduct; and provide training and counseling, as appropriate.

Title VII applies to local governments and prohibits the use of interview screening measures that have the effect of excluding individuals of a protected class disproportionately, unless that screening method can be justified as a business necessity (e.g., a requirement that an applicant have the ability to carry 75 pounds might disproportionately exclude women, but may be permissible if necessary for the job). Questions of employees or applicants relating to national origin, religion, political affiliation

or other personal characteristics protected by the civil rights laws are to be avoided. Since questions regarding such matters rarely, if ever, are job-related, the fact that the questions were asked might be used by an employee as evidence that the employer took such factors into account when making employment decisions.

Similarly, the *Americans with Disabilities Act* (ADA), 42 U.S.C. § 12101, et seq., which covers many private and municipal, but not state, employees, prohibits questions regarding an applicant's disability prior to the making of a job offer. The ADA may also come into play with respect to potential screening of individuals who have suffered a serious physical or emotional impairment as a result of acts of vandalism, terrorism or fears of future terrorist events. The ADA further limits the types of medical examination that can be required of post-offer hires and employees.

Beyond restrictions on questioning of employees and applicants, Title VII also imposes a duty upon employers to prevent a hostile work environment, where harassment of employees based upon their race, religion, sex, or national origin occurs. Harassment, according to the EEOC, is a form of discrimination that may violate Title VII of the *Civil Rights Act of 1964*, the *Age Discrimination in Employment Act of 1967*, and the *Americans with Disabilities Act*.

Employees may become suspicious of other employees or contractors and may engage in harassment or workplace violence against others in a protected class. As a general matter, Title VII of the Civil Rights Act requires covered employers to train managers and employees to ensure a nondiscriminatory, non-hostile work environment and to promptly investigate and remedy instances of discrimination or harassment in the workplace. Employers should evaluate whether they have a comprehensive Equal Employment Opportunity and Complaint procedure that is distributed to all employees. This action is particularly encouraged as the employer is automatically liable for proven harassment by a supervisor resulting in a negative employment action such as failure to promote or hire, loss of wages and termination. In the event that the supervisor has created a hostile work environment, the employer is limited in its ability to avoid liability. Therefore, where complaints of discrimination or harassment occur—whether involving supervisors, co-workers or vendors—employers should consider whether they have an effective process for promptly investigating and remedying these situations as appropriate. Owners and operators of water resources facilities may need to re-examine their procedures for preventing workplace violence or taking disciplinary action against perpetrators of harassment or violence. If there are indications that violence may occur, municipal water and wastewater treatment agencies may wish to take special precautions, such as preventing employees from bringing weapons or firearms on-site unless they are needed to perform their jobs.

The EEOC received 23,034 charges of alleged harassment in fiscal year 2006; 22,408 of these charges were administratively resolved allowing the EEOC to recover $59.08 million in monetary benefits, exclusive of monetary benefits recovered through litigation. These figures demonstrate the prevalence of alleged harassment in the workplace, emphasizing the need for employers to act diligently in addressing these concerns.

Questions about eligibility for a position with a water sector facility implicate not only civil rights laws per se, but immigration law issues that require employers to establish work eligibility at the

commencement of employment, obviating a need to gather this information at a later date. See 8 U.S.C. § 1324a.[84] *The Immigration Reform and Control Act of 1986*, and the *Immigration Act of 1990*, as well as the governing regulations, prohibit public and private employers from knowingly hiring, recruiting or referring "unauthorized aliens" for employment, and impose significant penalties for violations of the Act. The requirement that employers not hire individuals without work authorization extends to existing employees as well. Therefore, if an employer learns that an existing employee is not authorized to work lawfully in the United States, it must terminate the employment relationship. The employer may – but need not – notify immigration authorities if the relationship is ended, as long as notification is done in a consistent and nondiscriminatory manner.

While the federal government generally requires citizenship for civil service positions in the Executive Branch, questions regarding citizenship posed to applicants for local government positions may raise legal issues. Questions regarding citizenship, as opposed to questions regarding eligibility to work, may form the basis of a later discrimination claim. Some states and local governments either allow or disallow questions related to citizenship based on the sensitivity of the position.

Private water sector employers generally have more latitude than public employers when screening applicants and managing their workforce, but, for the most part are still subject to the requirements of civil rights statutes. In addition to federal discrimination legislation, anti-discrimination requirements are contained in state statutes and even clauses in local ordinances and charters.[85]

2. Civil and Criminal Background Checks

Many states and municipalities have detailed selection procedures designed to ensure standardization of processes, validation of employment decisions, and nondiscriminatory implementation of requirements. Given the variability from state to state, and from one local jurisdiction to another, employers should always consult local requirements. As a general rule, employers may lawfully conduct background checks on applicants, including checking an applicant's references, verifying an applicant's current and previous addresses, confirming an applicant's prior employment and educational history, and verifying facts through public records. To ease the process of checking applicant references, employers can, depending on local requirements, include a waiver on the application by which the applicant agrees to allow his or her former employers to discuss his previous employment with the prospective employer.

Many employers would argue that comprehensive background information, including the criminal records of job applicants, are universally relevant for any positions filled in the water sector. However, some commentators have questioned criminal background checks as an adequate predictor of potential terrorist threats, noting that none of the 9/11 hijackers attempted to bypass legal procedures to enter the United States; instead they exploited the legal entry systems.[86] State and local requirements ideally should be consulted before conducting the check. If background checks are performed for positions, the employer should consider doing them for all applicants, or all applicants for particular positions, to ensure consistency and fairness.

In a majority of states, criminal background checks to disclose convictions can be performed on current employees consistent with the requirements of the *Fair Credit Reporting Act*. Employee

screening measures can implicate legal liability under the *Fair Credit Reporting Act*, 15 U.S.C. § 1681. This Act, enforced by the Federal Trade Commission, requires employers to provide written disclosure to an employee and obtain written authorization of the employee prior to obtaining credit or other reports from consumer reporting agencies. For example, employers must make certain disclosures whenever they ask a consumer reporting agency to assemble an "investigative consumer report" on employees. An "investigative consumer report" is any "report or portion thereof in which information on a consumer's character, general reputation, personal characteristics, or mode of living is obtained through personal interviews with neighbors, friends, or associates of the consumer reported on or with others with whom he is acquainted or who may have knowledge concerning any such items or information." 15 U.S.C. § 1681a(e). Again, state laws might bear directly on this issue as well.

Employers filling sensitive security positions within publicly owned water supply or wastewater treatment systems generally have greater latitude to screen and demand information of applicants and employees than when filling other more routine positions. While it may strike some as axiomatic that security-related positions should not be open to those with criminal records beyond minor offenses, state laws may regulate whether, and to what degree, an individual's criminal history can be considered in hiring. For example, before using a conviction in the hiring process, New York public and private employers must consider several elements including the age of the person at the time of the offense, time elapsed since the occurrence, and the bearing, if any, the criminal offense or offenses for which the person was previously convicted will have on his/her fitness or ability to perform one or more of such duties or responsibilities. N.Y. Correct. Law § 753.[87] In some states, employers are not permitted to include questions about "arrest records" on applications or during interviews.[88]

A minority of states prohibit employment discrimination on the basis of arrest records for certain types of offenses and/or criminal convictions that are not germane to the position applied for or held, including but not limited to Massachusetts, Michigan, and New York. See, e.g., N.Y. Correct. Law §§ 750, et seq.;[89] Mass. Gen. Laws Ch. 151B, § 4 and Ch. 276, § 100A. Some states further prohibit the use of psychological stress evaluator examinations, i.e. polygraph examinations. See, e.g., Mass. Gen. Law. Ch. 149, § 19B;[90] Mich. Comp. Laws Ann. § 37.203; N.Y. Lab. Law § 735. Massachusetts has developed a Criminal Offender Record Information System (CORI) that enables employers to obtain information through a "public access record check" only if an individual has been convicted of a crime punishable by five years in prison or the offender is currently incarcerated or has been recently released. Mass. Gen. Laws ch. 6, §§ 168, 172. If an individual does not fit this profile, the employer must apply for "special certification" from the Criminal History Systems Board to receive an offender's complete record, which requires a two-thirds vote that "the public interest in disseminating such information to these parties clearly outweighs the interest in security and privacy" in order for such a request to be granted. § 172(c). These types of requirements vary depending on the state and municipality and should therefore be consulted.

Determining whether or not to screen applicants by comparing their names to government-issued lists of individuals wanted for questioning in regard to possible terrorist activity, for example, has potential liabilities whichever choice is made. Employers with access to such a list that do not check to see if applicants appear on such a list run the risk that if a listed applicant were hired, and then committed a crime, the failure to check the lists could serve as the basis of a negligent hiring cause of action, a tort which has been recognized in some states. See, e.g., *Detone v. Bullit Courier Serv., Inc.*,

140 A.D.2d 278, 528 N.Y.2d 575 (1988)[91] (New York law); But see *Freeman v. Adams Mark Hotel*, 2004 WL 1811393 (W.D.N.Y. Aug 13, 2004) (NO. 01-CV-768A); See also *Tallahassee Furniture Co. v. Harrison*, 583 So.2d 744 (Fla. 1st DCA 1991) (Florida law); But see *Staten v. Ohio Exterminating Co., Inc.*, 123 Ohio App.3d 526, 704 N.E.2d 621 (Ohio App. 10 Dist. Nov 04, 1997) (NO. 97APE04-529).[92]

In negligent hiring or retention cases, liability often turns on whether or not it was reasonable for the employer to permit the employee to perform their job, taking into account the information that the employer knew or should have known about the employee. *Detone* stands for the proposition that negligence is not presumed as it must be proven by a preponderance of the evidence by the plaintiff. Additionally, in order to demonstrate employer negligence, it must be proven that the employer placed the employee in foreseeable harm which would have likely spared *the injured party had the employer taken reasonable care in making decisions respecting the hiring and retention of his employees.*[93] In general, the test, set forth in *Tallahassee*, requires the employer to determine *whether or not they exercised the level of care which, under all the circumstances, the reasonably prudent person would exercise in choosing or retaining an employee for the particular duties to be performed.* [94]

Simply refusing to hire an applicant whose name appears, or is similar to a name that appears, on a watch list could violate Title VII as an employee screening mechanism that adversely impacts certain nationalities. Employers that use or maintain such lists also could potentially run afoul of state black-listing prohibitions; violation of some of these prohibitions may result in strict liability. See, e.g., Ala. Code § 13A-11-123; Me. Rev. Stat. Ann. Tit. 17 § 401. However, employers are probably justified in requiring an additional inquiry into the background of any listed applicant, including whether the applicant had or was willing to cooperate in the governmental investigation, and whether he or she remained the subject of an investigation.

3. Monitoring Employees at the Workplace and the USA Patriot Act

This is an emerging area of the law and judicial decisions are varied. In addition to the state and local statutory and regulatory requirements identified above, certain theories of employee privacy are emerging from the common law of privacy; from certain statutory privacy rights (including in the areas of electronic communications, medical information, credit information, and polygraph testing); and from federal and state constitutions. For example, while an individuals' personal communication is protected against government surveillance conducted without a court order by the *Electronic Communications Privacy Act*, (ECPA) of 1986, there appears to be very little privacy protection of employees from communications conducted on employer-owned equipment.

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (*Patriot Act*)[95] has expanded the government's ability to monitor corporate, private, and government activity and communications in an effort to thwart terrorism. The *Patriot Act's* sweeping provisions cover such wide-ranging topics as international money laundering, border protection, and compensation for victims of terrorism and their families. Congress' express goal in passing the *Act* was to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes.[96] The *Patriot Act* enhances the federal government's surveillance authority, but it does not delegate these new authorities to municipalities.

The *Patriot Act* imposes specific responsibilities on financial institutions requiring them to "know their customers" in an effort to prevent any money laundering or similar activities that may finance terrorism and narcotics trafficking. In an effort to screen potential and current employees, the employing financial institutions are expressly authorized to use various terrorist search databases. While some of these search resources are government based, it is imperative that employers are aware that the *Fair Credit Reporting Act* (FCRA) constrains all employment screening and requires reasonable procedures to be used in an effort to maximize privacy and accuracy. Additionally, FCRA does not allow background screenings that violate any state or federal anti-discrimination laws. Furthermore, employers should take into account errors in such databases and understand that listed persons may take measures to hide their true identity. Understanding the *Patriot Act's* reach with respect to financial institutions does not leave the water resources sector immune from other *Patriot Act* obligations.

Title II of the *Patriot Act* applies to water sector infrastructure and to public and private activities more generally. Title II focuses on enhancing surveillance procedures, coordinating intelligence, and gathering evidence necessary to execute warrants and institute criminal proceedings, while also broadening the government's wiretapping and computer surveillance capabilities. Title II further gives the government authorization to conduct secret searches of homes and offices, and it grants increased access to financial, business, medical, and educational records. It is imperative that employers familiarize themselves with these new requirements to strike the necessary balance between the government's information need and their employees' privacy interests. The *Patriot* legislation does not impose specific responsibilities governing municipalities or their contractors and employees. However, to the extent that current and pending legislation is increasingly cautious in regard to potential terrorist activity, it may be considered a factor in determining whether water sector facilities have exercised reasonable care with respect to their employees.

Certain monitoring of existing employees also is permissible. For example, while employers routinely monitor their employees' use of employers' electronic communication equipment, such monitoring ideally is undertaken with extreme care and with notice to employees of such monitoring through a comprehensive and effective Electronic Communications Policy. In addition, many employers are engaging in video surveillance of their employees in order to combat workplace theft, violence and misconduct. Visible, closed-circuit video cameras generally will be found lawful, particularly where they are deployed in work areas and employees are given advance notice of their use.

In monitoring existing employees, employers should not create a hostile workplace environment. Hidden cameras of which employees have no notice are problematic because their lawfulness often turns on whether the employees have a "reasonable expectation of privacy"[97] in the area in which they were videotaped. Camera surveillance of elements of a nation's infrastructure have become commonplace, although somewhat controversial because of privacy concerns. The investigation of, and emergency response to, the recent terrorist attacks on London's underground transportation system were aided by use of surveillance cameras in public areas. What is a "reasonable expectation of privacy" in public places is shaped by the threat of terrorist activity. Utilities may assert that monitoring is essential not only to security in many areas of water sector facilities, but also to safety and efficiency of operation.

In *Nelson v. Salem State College*, 446 Mass. 525, 845 N.E.2d 338 (Mass. 2006), a state college employee was videotaped by a hidden camera while changing her clothes and applying sunburn medication to her chest and neck in an open area of her workplace. The employee brought a § 1983 claim and an invasion-of-privacy claim against the college and college's public safety officers. The court held that there was "no objectively reasonable expectation of privacy in [the employee's] workplace" for purposes of her § 1983 Fourth Amendment privacy claim, and additionally, the officers were "shielded from liability by the doctrine of common-law immunity" with respect to the employee's invasion of privacy claim."[98]

Although courts have upheld employer searches of such things as employee work stations and lockers, the decisions generally are determined on a case-by-case basis, often turning on whether the employee was on notice of a possible search, whether the employee had a reasonable expectation of privacy in the area, and whether the practice was undertaken in a nondiscriminatory manner. Case law demonstrates that a determining factor in most employee privacy litigation is the reasonableness of an employee's expectation of privacy. The requirement that there is a reasonable expectation of privacy is derived from the Fourth Amendment to the United States Constitution. Employers generally are well advised to let employees know that the employers' policies include particular surveillance measures, such as the possibility of locker searches. In addition, municipal employers will need to decide how much information to provide voluntarily. Ordinarily, it will not be problematic to share general information with law enforcement officers informally, such as dates of employment, addresses, phone numbers, so long as protected information—such as medical information—is not revealed and the procedure is followed consistently for all employees. Municipal employers can ask the requesting agency if they can seek the employee's permission before providing the information. If they cannot obtain the employee's permission or if the request is for information that the employer is uncomfortable providing voluntarily (such as more detailed information, or for access to the work-site), municipal employers may request service of legal process which will legally obligate the employer to provide the requested information and will provide some protection from common law tort liability.

If an employee is jailed, or accused of criminal activity, does the municipal water or wastewater authority have any specific obligations to the employee? Some municipal ordinances provide indemnification or surety for directors and certain employees for conduct in the normal course of business. See *e.g.*, City of Indianapolis Ordinance Title I, Ch. 292.[99] Such ordinances generally do not, however, provide such indemnification for criminal, malicious, or wanton activities. *Id.* However, some agency by-laws may provide broader protection and cover the cost of defense for officials and their employees, as well as the cost of investigation, for criminal or civil matters. If the action results in a conviction the individual must reimburse the agency. See *e.g.*, Article XIII, By-Laws of Metro Wastewater Reclamation District, Denver, CO, Republished Dec. 17, 1997.

If an employee is the target of investigation because of suspected terrorist activity, the water sector agency should follow normal procedures for cooperating with law enforcement agencies. During the investigation, it may be prudent to place the employee on administrative leave. Issues regarding the negligence of the water sector authority may arise out of activity that causes injury. In addition, certain types of criminal activity can be imputed to entities for acts of their employees, although this

is normally limited to instances where the activity is within the duties of the employee and is tacitly sanctioned by the entity.

It is important to note that municipal water and wastewater treatment agencies may be held criminally liable for the acts of their employees. Under the "collective knowledge" doctrine, the employees' collective knowledge and intent can be used to hold the employer liable even where no individual criminal liability would exist. Criminal liability of employers can even be found even where an employee's conduct is in direct violation of the employer's policy or directions, where directions were not communicated diligently or enforced. In addition, virtually all federal environmental statutes include criminal liability provisions that attribute criminal acts of a "responsible official" to his or her employer. Thus, municipal water sector agencies would be wise to seek advice of counsel to assess whether alleged criminal actions of an employee might implicate the agency.

CHAPTER ENDNOTES

66 NRC, *Improving the Nation's Water Security: Opportunities for Research* at 21 (Feb . 27, 2007).

67 Id.

68 Id.

69 The current debate on what information should be released or held exempt from disclosure is epitomized by the debate over the Department of Homeland Security's efforts to keep such information confidential. The ABA has taken a pro-disclosure position related to "sensitive but unclassified" information gathered by DHS. See Resolution of The ABA (February 13, 2006), while the Administration has generally backed withholding of such information, even when a *Freedom of Information Act* request is received.

70 U.S. Department of Homeland Security & U.S. Environmental Protection Agency, *Water: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan* (May 2007) at 46-59; 100-101.

71 See 42 U.S.C. § 300i-2(a)(3); U.S. Environmental Protection Agency, *Protocol to Secure Vulnerability Assessments Submitted by Community Water Systems to EPA* (Nov. 2002).

72 Id.

73 Chemical Facility or facility shall mean any establishment that possesses or plans to possess, at any relevant point in time, a quantity of a chemical substance determined by the Secretary to be potentially dangerous or that meets other risk-related criteria identified by the Department. However, proposed interim final rule 6 CFR § 27.110 exempts water suppliers and wastewater treatment facilities sector regulated under the *Clean Water Act* and the *Safe Drinking Water Act*.

74 Publication of specifications for bidding on construction of new facilities is another avenue of disclosure of sensitive information yet to be adequately addressed in the law. Some state statutes may directly touch on this issue, but most have not yet addressed the problem. It is best for water sector utilities concerned about sensitive disclosure in a bidding process to check their state law for any potential protections.

75 See 6 U.S.C. §131; Final rule found at 6 CFR 29.

76 More information regarding the PCII program can be found at http://www.dhs.gov/xinfoshare/programs/editorial_0404.shtm.

77 NRC, *Improving the Nation's Water Security: Opportunities for Research* (Feb . 27, 2007).

78 U.S. Department of Homeland Security & U.S.Environmental Protection Agency, *Water: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan* (May 2007).

79 NRC, *Improving the Nation's Water Security: Opportunities for Research* (Feb . 27, 2007).

80 Statistics as of June 20, 2007.

81 A copy of the Water SSP can be found on the DHS website at http://www.dhs.gov/xprevprot/programs/gc_1179866197607.shtm.

82 Information on the EMAC is available at http://www.emacweb.org/index.cfm; WARNs are organized on the state level and utilities wanting more information should contact their state department of emergency response for more information on the availability of a state WARN. Information on existing WARNs and how to develop a WARN can also be found on WaterISAC at www.WaterISAC.org.

83 Sex includes pregnancy, childbirth and related medical circumstances. See Title VII of the *Civil Rights Act* (Title VII), 42 U.S.C. § 2000e et seq. and the *Age Discrimination in Employment Act* (ADEA), 29 U.S.C. § 621 et seq. ADEA protects individuals over the age of forty from age based discrimination, articulating specific guidelines for pension, benefit and retirement plans.

84 There are proposed legislative amendments to this statute pending.

85 See, e.g., City Code of Stamford, CT, Chapter 47, Art. VII, § 47-23.

86 See *The National Commission on Terrorist Attacks Upon the United States* at http://www.9-11commission.gov/staff_statements/staff_statement_1.pdf.

87 There have been recently proposed amendments to this law: 2007 NY S.B. 1602 (NS), 2007 New York Senate Bill No. S1602, New York Two H, (Jan 23, 2007) VERSION: Introduced, PROPOSED ACTION: Amended.

88 In addition, employers should recognize that making pre-offer inquiries into the medical condition of an applicant or questioning the prior history of workers' compensation claims may raise ADA claims or be prohibited by state law. Any condition inquired about must relate to a bona fide occupational qualification.

89 This statute currently reads: "No application for any license or employment, to which the provisions of this article are applicable, shall be denied by reason of the applicant's having been previously convicted of one or more criminal offenses, or by reason of a finding of lack of 'good moral character' when such finding is based upon the fact that the applicant has previously been convicted of one or more criminal offenses, unless:
(1) there is a direct relationship between one or more of the previous criminal offenses and the specific license or employment sought; or
(2) the issuance of the license or the granting of the employment would involve an unreasonable risk to property or to the safety or welfare of specific individuals or the general public."

90 This Massachusetts law is a useful reference because it specifically outlaws "lie-detector" tests:
"It shall be unlawful for any employer or his agent, with respect to any of his employees, or any person applying to him for employment, including any person applying for employment as a police officer, to subject such person to, or request such person to take a lie detector test within or without the commonwealth, or to discharge, not hire, demote or otherwise discriminate against such person for the assertion of rights arising hereunder. This section shall not apply to lie detector tests administered by law enforcement agencies as may be otherwise permitted in criminal investigations." Id. at 19B(2).

91 This case has received some negative history but has not been overruled, See *Freeman v. Adams Mark Hotel* 2004 WL 1811393, *1 (W.D.N.Y.) (W.D.N.Y., 2004).

92 This case has received some negative history but has not been overruled, See *Staten v. Ohio Exterminating Co., Inc.* 123 Ohio App.3d 526, *531, 704 N.E.2d 621, **624 (Ohio App. 10 Dist.,1997) *Detone v. Bullit Courier Service, Inc.* 140 A.D.2d 278, *279 -280 (N.Y.A.D.,1988).

93 Id.

94 *Tallahassee Furniture Co., Inc. v. Harrison* 583 So.2d 744, *750 (Fla.App. 1 Dist., 1991).

95 *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (U.S.A. Patriot Act), as amended and reauthorized, 18 U.S.C. § 1(2007).

96 Id.

97 Drawn from the Fourth Amendment to the United States Constitution's search and seizure clause.

98 *Nelson v. Salem State College*, 446 Mass. at 525.

99 The revised Code is available at: http://www.municode.com/resources/gateway.asp?pid=12016&sid=14.

Chapter 5

Liability for Releases of Hazardous Materials as a Result of an Act of Terrorism or Vandalism

Liability for Releases of Hazardous Materials as a Result of an Act of Terrorism or Vandalism

A. Substantive Federal Environmental Law Causes of Action Applicable to a Release of Hazardous Materials or Substances as a Result of an Act of Terrorism or Vandalism

There are many federal and state regulatory requirements applicable to potential releases of hazardous substances, such as chlorine or ammonia, into the environment. Entities that possess or emit/discharge these types of substances are required by federal law to develop plans to prevent such incidents and to respond to releases that do occur under the *Resource Conservation and Recovery Act* (RCRA). If releases do occur, litigation may be commenced by governmental authorities or members of the public to enjoin the release or to penalize operators for the releases.

The collapse of the World Trade Center towers on 9/11 generated a cloud of debris that coated the surrounding buildings and streets of Lower Manhattan with concrete dust, asbestos, lead, and other building materials. Fires within the wreckage burned for months, emitting various metals and particulate matter in addition to such potentially harmful substances as dioxin, polychlorinated biphenyls (PCBs), volatile organic compounds (VOCs), and polycyclic aromatic hydrocarbons. *Lombardi v. Christine Whitman*, 2007 U.S. App. LEXIS 8961, *2 (2d Cir. April 19, 2007). In *Lombardi*, the plaintiffs brought suit on November 23, 2004, in the Southern District of New York, on their own behalf and on behalf of a purported class including all those who worked at or in the immediate vicinity of the site during the period September 11, 2001, to October 31, 2001, without sufficient respiratory equipment, purportedly in reliance on information supplied by government officials, and who as an alleged result suffer or reasonably fear suffering illness or injury from their exposure to asbestos or other harmful substances.

The defendants, sued in their individual capacities, are current or former officials of the Environmental Protection Agency (EPA), the White House Council on Environmental Quality (CEQ), and the Occupational Safety and Health Administration (OSHA). The claims against them are based on statements in EPA press releases issued in the wake of the disaster, which (according to the complaint) were made (1) to speed work at the site, (2) with the knowledge they were false or misleading, and (3) with deliberate indifference to the health risks the workers would incur by relying on them. Both the Federal District Court and the Second Circuit held that first responders at the WTC, who worked with scant respiratory protection, had failed to state a claim upon which relief could be granted. *Lombardi v. Christine Whitman*, 2007 U.S. App. LEXIS 8961, *35 (2d Cir. April 19, 2007).

Water sector owners and operators are generally aware of the applicable environmental regulations covering their facilities, but may not have fully considered the extent to which these requirements and potential liabilities are affected by whether a release is caused by an act of terrorism, vandalism, or other event that was extremely unlikely to occur prior to September 11th. As evaluated in detail previously, releases may also give rise to common-law tort causes of action based on personal injury or damage to property.

The following discussion summarizes federal provisions that the U.S. Department of Justice and private citizens could rely upon in pursuing litigation against water sector facilities following a terrorist attack and resultant hazardous releases.

1. Potential Liability Under CERCLA (Superfund)

The obvious starting point for the discussion of liability for releases of hazardous materials is the *Comprehensive Environmental Response, Compensation and Liability Act* (CERCLA) or "Superfund" law. 42 U.S. C. § 9601 et seq. None of the federal environmental statutes, with the exception of the right of cost recovery or contribution for private clean-ups of hazardous releases under the CERCLA, creates any private right of action for personal damages from hazardous substances or pollutants. In fact, the U.S. Congress rejected efforts to create a private right of action for injuries when the 1980 Superfund law was enacted.

Nevertheless, the limited citizen suit provisions of CERCLA have been used in litigation following terrorist attacks. These recent lawsuits indicate that water sector facilities should be aware of the possibility that plaintiffs will continue to attempt to bring claims based on a variety of environmental statutes when terrorism strikes.

In *Benzman v. Christine Whitman*, 2006 U.S. Dist. LEXIS 4005 (S.D. N.Y. 2000), the plaintiffs were residents of Lower Manhattan and Brooklyn; students attending schools in Lower Manhattan and Brooklyn; and workers whose place of employment was in Lower Manhattan and Brooklyn, all of whom had been exposed to hazardous substances in the interior of their residences, schools, and workplaces as a result of the dust and debris released from the collapse of the WTC towers and surrounding buildings following the terrorist attacks on 9/11. Plaintiffs brought a class action grounded upon four causes of action against EPA and named government officials.[100] Count Four was brought pursuant to the citizen suit provision of CERCLA, 42 U.S.C. § 9659(a)(1), for alleged violation of regulations under CERCLA. The causes of action sought identical relief: to compel testing by the EPA of office buildings, schools and residences in Lower Manhattan and Brooklyn, and if such tests reveal the presence of hazardous substances, to implement a professional clean-up of all such buildings, and to compel the EPA to implement a program for medical monitoring. Plaintiffs also sought compensatory damages, reimbursement of costs incurred by Plaintiffs, and the creation of a fund to finance medical monitoring services. The EPA, as the sole defendant named in the fourth cause of action, moved to dismiss that claim on the ground that Plaintiffs had failed to properly allege a CERCLA citizen suit claim. CERCLA's citizen suit provision permits citizens to sue as private attorneys general in circumstances where government authorities have, after given notice, failed to take steps to remedy certain environmental harms. Section 9659 provides that:

> **(a) Authority to bring civil actions except as provided in subsections (d) and (e) of this section and in section 9613(h) of this title (relating to timing of judicial review), any person may commence a civil action on his own behalf**
>
> > **(1) against any person (including the United States and any other governmental instrumentality or agency, to the extent permitted by the eleventh amendment to the Constitution) who is alleged to be in violation of any standard, regulation, condition, requirement or order which has become effective pursuant to this chapter . . .; or**

> **(2) against the President or any other officer of the United States (including the Administrator of the Environmental Protection Agency and the Administrator of ATSDR) where there is alleged a failure of the President or of such other officer to perform any act or duty under this chapter, including an act or duty under section 9620 of this title (relating to Federal facilities), which is not discretionary with the President or such other officer. 42 U.S.C. § 9659(a).**

The Court noted that Plaintiffs' allegations against the EPA were for alleged failures to carry out its duties under CERLCA as administrator of CERCLA, and not as a regulated party: "The EPA, as administrator of CERCLA, does not regulate itself." While dismissing the complaint for improper venue, the court noted that "the appropriate citizen suit provision for the types of allegations made by Plaintiff here is § 9659(a)(2)." Thus, while dismissing the CERCLA count, the Court, in dicta, acknowledged that a CERCLA count could have been brought by the citizen plaintiffs in the appropriate venue in Washington, DC.[101]

While the suit was unsuccessful, water sector facilities may be liable for injunctive relief and other corrective action under the federal environmental laws and their state counterparts if hazardous substances were released into the environment as the result of terrorist activity or vandalism. An owner or operator of a water resources facility may also be held liable under Superfund for the clean-up costs associated with a release of any quantity of hazardous substances from the facility into the environment. 42 U.S.C. §§ 9606; 9607(a); 9613. Neighboring landowners also can sue for clean-up costs they incurred as a result of the release, including costs associated with investigating, mitigating and/or remedying the release. In addition, if the resulting contamination is severe enough to warrant the inclusion of a location on EPA's National Priorities List, the government can initiate a clean-up of the site, sue to recover its response costs or bring suit to enjoin the agency to undertake the clean-up itself. The United States may also obtain compensation for natural resource damages resulting from the release. 42 U.S.C. § 9607(a).

The likelihood of the United States pursuing such actions following a terrorist attack is probably increased if a facility has conducted a vulnerability assessment and failed to pursue appropriate corrective action. Defenses to a terrorist incident under Superfund may include an "act of war" under 42 U.S.C. § 9607(b)(2). The "act of a third party" defense also may be available; to assert it, however, the facility must be able to prove that it exercised due care with respect to the hazardous substance concerned, and that it took precautions against foreseeable acts. 42 U.S.C. § 9607(b)(3). See *e.g., U.S. v. Conservation Chemical Co.*, 619 F. Supp. at 203 (W.D. Mo. 1985). Note that these defenses are affirmative and are unavailable if the third party is an agent, an employee, or an independent contractor of the facility. See *e.g., U.S. v. Ward*, 618 F. Supp. 884 (E.D.N.C. 1985). The third party defense is likely to be invoked by wastewater facilities or owners who are forced to discharge contaminated water following a terrorist attack on a chemical plant or other industrial facility that discharges to treatment plant under the *Clean Water Act* pretreatment program. 33 U.S.C.§1317.[102]

2. Potential Clean Water Act Liability

The EPA Administrator or citizens may bring suit against any water sector facility that has violated effluent limits in its NPDES permit or stormwater discharge permit. 33 U.S.C. § 1311. Fines of up to

$32,500[103] per day may apply. 33 U.S.C. § 1319. Water sector facilities would also be liable for spills of oil and hazardous substances into waters of the United States. 33 U.S.C. § 1321. In the event of a terrorist attack directed at a wastewater treatment facility that results in a release of pollutants that exceed NPDES permit limits, the facility, if sued by the government, would in all likelihood invoke an "act of war" defense. Similarly, if a water treatment plant, chemical plant, or other industrial facility is attacked, indirectly causing the treatment plant to release pollutants to the environment, an "act of war" and the "third party defense" just described above would likely be invoked. In regard to other suits, since citizens may not sue for wholly past violations under the *Clean Water Act*, they may not have standing to sue for a one-time act of terrorism or vandalism.

3. Potential Clean Air Act Liability

Under Section 303 of the *Clean Air Act*, injunctive relief is available to address emissions that present an imminent and substantial endangerment. Moreover, water sector facilities may be civilly or criminally liable for the release into the air of any hazardous air or any *Emergency Planning and Community Right-to-Know Act* (EPCRA) Extremely Hazardous Substance (EHS) if the municipal water or wastewater authority has placed any person in imminent danger of death or serious bodily injury. See, 42 U.S.C. § 7413(c)(4). In addition, any water sector facility that is permitted under Title V of the federal *Clean Air Act* is liable for any emissions that violate its permit limits.

B. Substantive State Causes of Action for Releases of Hazardous Substances as a Result of a Terrorist Attack

1. Potential Liability Under State Environmental Statutes

Since the 1970's, when kepone was released into the James River in Virginia, and methyl isocyanate releases occurred at Union Carbide's West Virginia plant, the issue of private recoveries from companies under state constitutions and state environmental laws has been a significant issue. Generally such laws create no private right of recovery to individuals suffering either property damage or personal injury. In certain instances, suits have been filed citing provisions in state constitutions establishing a state policy to protect its atmosphere, lands, and waters from pollution, impairment, or destruction, for the benefit, enjoyment, and the general welfare of the people of the state. See, e.g., Va. Const. art. X, § 1; Ill. Const. art. XI, § 2; N.Y. Const. art. XIV, § 4. Courts have held generally that such provisions do not create substantive rights enforceable by private individuals against either the states or other public entities operating in the state.

Like federal pollution control acts, state statutes rarely provide for private compensation for personal injuries. Note there are exceptions to this rule for property damages. For instance, certain states have "takings" laws which may facilitate claims for property damage or diminution in value of private property from the presence of hazardous substances. Certain local laws may provide compensation for damage to fish or other fauna, although these generally are not private rights of action. Nonetheless, since this is an evolving area of the law, if there were a release into the environment by a water sector facility, it may be important to evaluate whether such rights have been created in particular jurisdictions. In such cases, like the federal Coal Miner's Compensation Fund, State

Tobacco Funds or Worker's Compensation laws, the existence of an administrative compensatory mechanism generally may only be exercised if the claimant releases other claims against potentially responsible entities based on common law. There may be exceptions to Worker's Compensation laws, however, when an employee is the victim of a violent act in the workplace.

2. Potential Liability Under State Common Law Principles

Common law actions for a release of hazardous materials or substances as a result of an act of terrorism or vandalism may also be available. Tort law affords numerous bases at common law for personal claims for damages attributable to personal injury, diminution in value to property, and increasingly, fear of injury from exposure to hazardous substances. Most claims are based on negligence, trespass, or private nuisance.

a. Negligence

Negligent failure to secure a facility from a foreseeable terrorist attack is dealt with in detail in Section II. Numerous firemen, rescue workers, and police employed by the City of New York have suffered lung damage or respiratory illness allegedly from inhalation of asbestos and other hazardous materials at the World Trade Center site. A class action has been filed by such workers against the City of New York and its agencies. *In Re World Trade Center Disaster Site Litigation*, 456 F.Supp. 520 (S.D. N.Y. 2006). In that case, over 3,000 workers claimed permanent injury to their respiratory systems and their health and vitality, and a shortening of their lives. They claimed that the City and its contractors, and other Defendants, were negligent in monitoring the air and assuring appropriate safety in the workplace, particularly in not providing adequate respiratory equipment and assuring proper use of the equipment. Id. at 523. Ultimately this case should provide answers to many complex questions about municipal employer tort liability for employee injuries due to terrorist acts.

Water sector facilities, public or private, are generally held to a negligence standard in all their general operations: "Whether a water company may be held liable for damage or injuries arising from the operation of its water system depends, as in any other case, essentially upon a showing of the well-established elements of actionable negligence, such as knowledge or reasonable foreseeability, a duty to the person injured, a violation of such duty proximately causing the injury, etc. . . . Principles of negligence also govern questions of liability of a water company for injuries resulting from alleged impurity of the water which it furnishes." Oscar C. Sattinger, Liability for Injuries, 78 Am. Jur. 2d Waterworks and Water Companies § 59. See also *Gilette Shoe Co. v. City of New York*, 445 N.Y.S.2d 750 (N.Y. App. Div. 1982) ("The City does have a duty to exercise reasonable care in the maintenance of its water system."). While private individuals generally have no duty to protect or warn others against criminal attacks, courts may apply a different standard to owners of critical infrastructure.

To the extent that state laws and municipal charters impose a duty on plants to avoid actions posing unreasonable and foreseeable risk of injury to the public, a claimant might be able to argue negligence per se so that all he/she would need to prove is damages. Nonetheless issues in potential litigation are likely to be whether the particular danger was foreseeable and whether the

danger could have reasonably been guarded against. Whether contributory negligence is a bar to a claim or reduces the amount of recovery is jurisdiction specific.

b. Trespass

Claims in trespass or private nuisance are traditionally associated with the protection of property rights, but may still afford a means for obtaining compensation for exposures to environmental damages from a terrorist incident. Trespass is defined as an unlawful entry on the land of another causing some damage, no matter how negligible. Generally the plaintiff must establish that he has a possessory interest in the land and a physical invasion of that property resulted from the defendant's intentional or negligent action or is the result of an abnormally dangerous activity. The foreseeability of injury to another's property does not play a role in defending such a claim. Trespass actions, however, appear to have more limited application to personal injuries from exposure to toxic substances.

c. Private and Public Nuisance

In contrast to trespass, private nuisance does not focus on a tangible invasion of landowner's property so much as it hinges on the harm or annoyance imposed on others. Again, the plaintiff must establish a possessor interest and a substantial and unreasonable interference with his use or enjoyment of his property. Substantial damage awards for damage to health have resulted from public nuisance claims. See Prosser and Keeton, The Law of Torts, § 87 at 619 (5th Ed.). A claim based on public nuisance, generally defined as "any act or omission or use of property which is of itself hurtful to health tranquility or morals, or outrages the decency of the community," is a concept that most water sector facilities have historically contended with, and, although the plaintiff need not establish a particular private property interest, a private right of action generally can only be maintained when the plaintiff can show a substantial injury distinct from that suffered by the general public. The use of public nuisance owing to a terrorist incident is a potential but unproven ground for the recovery of damages.

C. Reporting Requirements in the Event of a Release

The entities that comprise the nation's water sector infrastructure are also well aware of the multiple federal, state and local requirements for maintaining plans to prevent releases of hazardous substances and reporting such releases when they occur. For example, they are aware of the need to prepare Risk Management Plans pursuant to *Clean Air Act* Section 112(r), 42 U.S.C. § 7412(r), and of the need to report accidental releases under Section 304 of the *Emergency Planning and Community Right-to-Know Act* (EPCRA), 42 U.S.C. § 1104. Recent attention to possible acts of eco-terrorism has heightened the importance of internal systems that assure compliance with these requirements and has raised questions about the need or desirability of re-evaluating current practices with respect to reporting incidents such as vandalism that may not have been reported routinely in the past because there may be no legal requirements to report them.

While not responsible for reporting suspicious incidents per se, if those incidents involve hazardous chemicals specifically, facilities are subject to various federal notice and reporting requirements that are triggered by the presence or the accidental release of certain hazardous chemicals over specific thresholds.

The various federal environmental notice and reporting requirements triggered by release are outlined in Table 1. Water sector facilities may also be subject to local ordinances and state laws that impose additional reporting requirements.

Violators of the federal reporting requirements can be liable for civil penalties of up to $32,500 per day, and knowing or willful violators can be subject to criminal penalties and/or imprisonment.

Water sector facilities may want to review their internal procedures to ensure that reporting and notice obligations are complied with, e.g., ensuring that a checklist of reporting obligations is available in several on-site locations for quick reference in the event of emergencies, and that records demonstrating compliance with these requirements are maintained on-site. It may be desirable to have copies of summaries of reporting obligations in several places on-site, and perhaps off-site, if an off-site repository is maintained for emergencies.

Table 1 – Summary of Federal Environmental Reporting Requirements

Authority	Notice or Reporting Requirement	Office to be Notified	Timing of Notice
42 USC § 11002, EPCRA § 302 (2007)	Facilities must give notice re: presence of an extremely hazardous substance (EHS) in excess of its threshold planning quantity (TPQ).[104]	SERC[105]	One-time notice.
42 USC § 11004, EPCRA § 304 (2007)	Owners/operators of facilities must provide immediate notice if a reportable quantity (RQ)[106] of an EHS or a CERCLA hazardous substance[107] is released over a 24 hour period, with certain exceptions.[108]	LEPC[109] SERC	Immediate notice upon release > RQ and written follow-up notice(s).
42 USC § 11021, EPCRA § 311 (2007)	Facilities that are required under OSHA's Hazardous Communication Standard to prepare or have available material safety data sheets (MSDS) for hazardous chemicals present on site must submit a list of those chemicals if they are present above a threshold amount.[110]	SERC LEPC Fire Dept.	One-time reporting obligation.
42 USC § 11022, EPCRA § 312 (2007)	Owner/operator must submit an annual inventory form re: amount of hazardous chemicals present at the facility during the preceding year, the average daily amount of hazardous chemicals on-site and location of those chemicals. Reporting is triggered if hazardous chemicals are present on-site above a threshold amount. (See EPCRA § 311).	SERC LEPC Fire Dept.	Submit Tier I/ Tier II Form annually on March 1.
42 USC § 9602, CERCLA § 103 (2007)	The "person in charge" of a facility must report any accidental release into the environment of hazardous substances over the RQ.	National Response Ctr. (NRC)	Immediate notice.
CWA 40 CFR 122.41(l)	NPDES permit holders must report any noncompliance with permit conditions that may endanger health or the environment.	State	Oral notice within 24 hours. Written submission within 5 days.

Authority	Notice or Reporting Requirement	Office to be Notified	Timing of Notice
CWA 40 CFR 117.21	The "person in charge" of a facility must report the discharge of a designated hazardous substance in quantities over the RQ that occur in any 24 hour period. [111]	NRC	Immediate notice.
42 USC § 7412, CAA § 112(r) RMP (2007)	If a facility has or uses a threshold quantity of a listed substance in a "process," that facility must develop and implement a risk management plan (RMP) and must maintain documentation of the program at the site. [112]	EPA	The RMP must be submitted by the date on which a regulated substance is first present above a RQ in a process, or 3 years after the date on which a regulated substance is first listed by EPA.
CAA § 112(r) "General Duty Clause"	Owners and operators of stationary sources that produce, process, handle or store EHSs have a "general duty" to ensure that the chemicals are managed safely, and must have a contingency planning process in place to minimize the consequences of any accident.	N/A	N/A

Water and wastewater systems are subject to CERCLA and the *Emergency Planning and Community Right to Know Act* for failing to report unpermitted releases into the environment. 42 U.S.C. 42 U.S.C. §§ 9601(10), 9603, 11004; 11046. The "person in charge" of a facility or system must immediately notify the National Response Center in the event of any accidental release into the environment of more than the reportable quantity of a hazardous substance. 42 U.S.C. § 9603; see list at 40 CFR § 302.4. The EPA Administrator may assess a penalty of not more than $25,000 per violation for failure to give notice of a release of an extremely hazardous substance under EPCRA or substances in excess of reportable quantities. For lists, see, 40 CFR § 355 App. A and B and § 302.4. The law also imposes prison sentences of not more than 2 years for knowing failure to notify state and local emergency response divisions of releases. 42 U.S.C. § 11045. Citizens may also bring suit under the citizen suit provision to enforce these requirements. 42 U.S.C. § 9659.

CHAPTER ENDNOTES

100 Count One alleged a violation of the Fifth Amendment of the Constitution. Count Two challenged EPA Defendants' actions after the September 11, 2001 attacks under the *Administrative Procedure Act* (APA), 5 U.S.C. § 701, et seq., as arbitrary and capricious, and contrary to Plaintiffs' Fifth Amendment rights. Count Three was a mandamus action, pursuant to 28 U.S.C. § 1361.

101 *See also Smith v. Potter, 208 F. Supp. 2d 415 (S.D.N.Y. 2002) aff'd. sub nom. APWU v. Potter*, 343 F.3d 619 (2d Cir. N.Y. 2003). In this recently-filed lawsuit, postal workers initiated litigation against the U.S. Postal Service asserting personal injury claims for damages from exposure to anthrax, based primarily on the federal Solid Waste Disposal Act, 42 U.S.C. 6901 et seq., and a claim that anthrax was an illegally transported hazardous waste. The case was dismissed.

102 Similar third party defenses are also likely to be raised in response to any negligence claim triggered by a discharge to treatment plant, which in turn releases contaminated water to the environment. See generally, Section II *infra.*

103 See 40 CFR 19.4.

104 The list of EHSs and their respective TPQs is published at 40 C.F.R. Part 355, Appendices A and B.

105 State Emergency Response Commission.

106 The RQs for EHSs are listed at 40 C.F.R. Part 355, Appendices A and B. The list includes ammonia and chlorine.

107 The list of CERCLA hazardous substances and their respective RQs is published at 40 C.F.R. § 302.4.

108 The following releases are exempt: (1) releases which result in exposure to persons solely within the boundaries of the facility; (2) federally permitted releases; (3) continuous releases if they are stable in quantity and rate; and (4) certain releases of pesticide products and radionuclides.

109 Local Emergency Planning Commission.

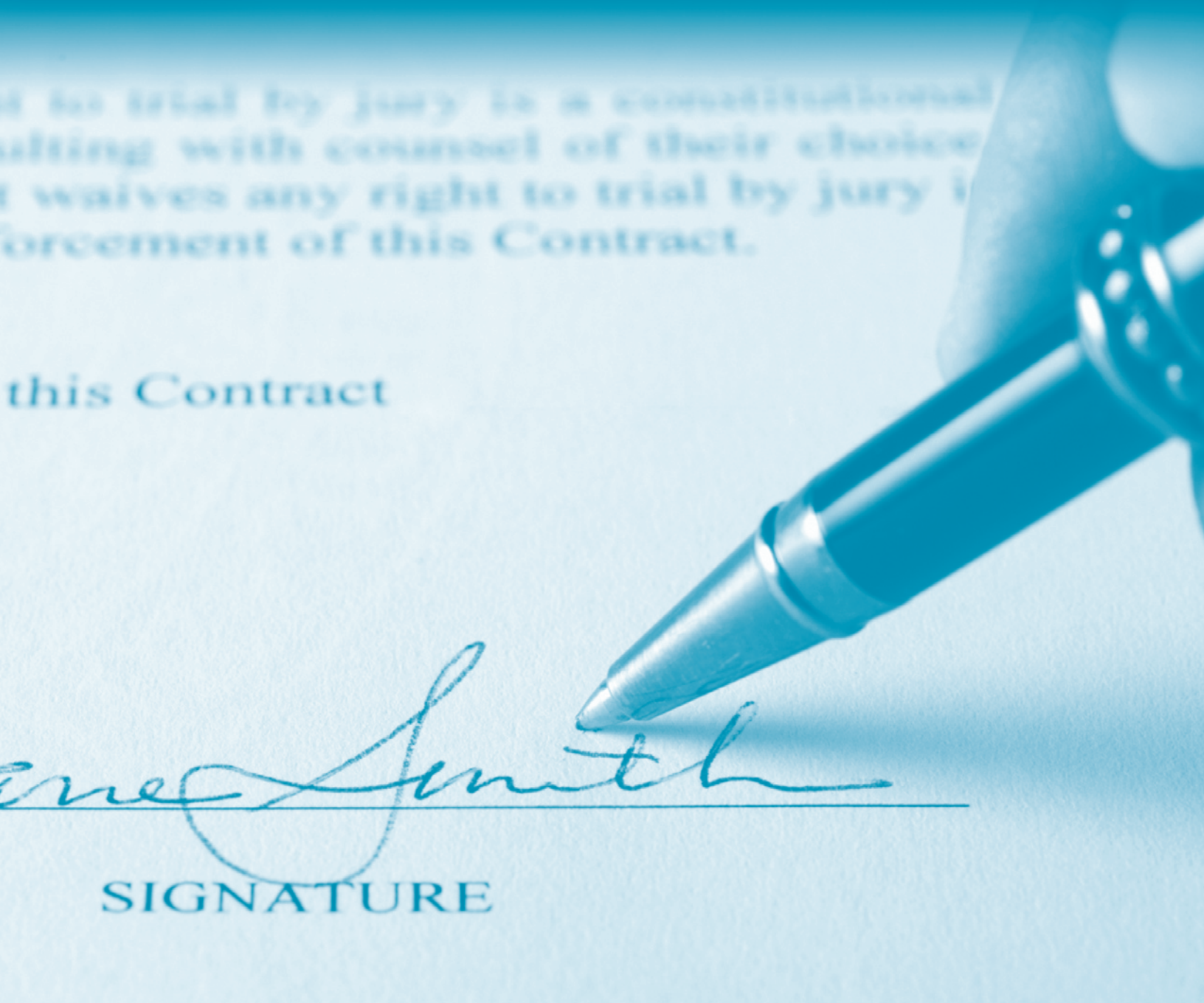
110 The threshold amounts for reporting are published at 40 C.F.R. § 370.20(b).

111 Designated hazardous substances and their RQs are listed at 40 C.F.R. § 117.3.

112 The list of threshold quantities and covered substances is found at 40 C.F.R. § 68.130.

Chapter 6

Contract Issues



Contract Issues

A. Contracting with Third Parties

Operators of water sector facilities that contract with third parties for services such as security, cleaning, or operation of chlorine tanks, biosolids removal or multi-year construction projects may not have considered the possible impact of acts of vandalism or terrorism when existing contracts were negotiated.[113] They may find it desirable to review existing contracts and/or to revise contracting procedures for entering into future agreements with the purpose of both providing greater security and of shifting liability to third parties in the event that an act of vandalism or terrorism occurs. Other issues such operators will confront relate to whether they have responsibilities with respect to security measures that their contract customers may, or may not, implement.

Recent events may lead operators to consider outsourcing to a greater degree than before. The system could be held vicariously liable, even criminally liable for acts of employees. There would be advantages to outsourcing; an operator is less likely to be found to be vicariously liable for any errors or omissions by the providers of outside services if it contracts with an independent contractor. However, owners and operators should bear in mind disadvantage could result from outsourcing, including less control over contractor security issues, unless these issues are/were negotiated with care before the contracts were executed.

Issues involving potential liability for third parties could arise if, for instance, it can be alleged that the authority failed to exercise care in selecting suppliers or vendors. It also is possible that similar claims could be made regarding personnel issues, especially if complaints have been lodged but not cured by the independent contractor, although it is very unlikely that a system could demand security checks of another employee's personnel.

As a normal rule, parties are bound by the terms of their existing contracts. However, by mutual consent, the parties can renegotiate the contracts to address new threats. Renegotiated terms may increase the cost of the contract to the municipal water resources authority that seeks to renegotiate.

In negotiating new contracts or contract renewals, an operator may wish to ask the other contracting party to bear the risk of damages associated with terrorist attacks. In appropriate circumstances, an operator may consider asking for indemnification from the other party. Contracts should also recite that the contracting parties are independent contractors, rather than employees, agents or subcontractors of the operator.

In the specific case of wastewater treatment facilities, legal requirements may exist for contract customers (such as industrial dischargers) under federal laws, common law, or local law—e.g., if the customer learns of a specific threat and fails to take action to investigate or prevent it. The contract customer may be bound by certain terms in the contract, which the wastewater treatment facility can sue on if the customer violates any of the terms. Additionally, many POTWs also have an industrial pretreatment program, which is required when certain types or volumes of industrial discharge are received by the treatment facility.[114] Under this program, the industrial discharger must "pretreat" its waste flow before discharging to the collection system or face penalties for noncompliance from an enforcement authority such as the

state. Such a pretreatment program provides the POTW with some legal protection against industrial dischargers and seeks to prevent environmental harm or damage to the treatment plant by preventing the discharge of pollutants which the plant is not equipped to treat. There may also be additional municipal ordinances or charters that place restrictions on customers discharging to POTWs, particularly if a failure on the part of its customer would affect the wastewater authority's discharge with regard to specific local water quality standards. The wastewater authority may often be empowered to enforce these local provisions.

Broad rights of entry for inspection, testing or other purposes are often included in municipal ordinances or charters. Some contracts with customers also may specify limitations on these broad rights such as the hours inspections may occur and the reasons for which they may be conducted (e.g., to inspect and sample wastewater discharge).

Certain enacting ordinances might be construed to allow service termination if a customer's influent threatens the integrity of a system or poses an imminent harm. On the other hand, proving that a customer is failing to exercise security responsibilities may require multiple inspections or observations to avert claims by the customer for damage.

B. Union Contracts

Owners and operators may utilize union labor in their facilities. Those that do so may have to work closely with union representatives to implement new security-related procedures, such as background checks or surveillance. Existing union contracts may have to be amended to allow for implementation of new security procedures.

In general, employers will need to consult existing collective bargaining agreements to determine their responsibilities to negotiate with union representatives prior to implementing any new policies and procedures. Employers that are subject to collective bargaining agreements may be required to bargain with representatives of employee unions prior to implementing policies which affect the terms and conditions of employment, and/or may be required to provide notice of such policy changes.

Employers likely will need to bargain with union representatives regarding changes in the terms and conditions of employment necessitated by a heightened security environment. These topics of bargaining may include increased security measures and changed hiring practices. Likewise, union representatives themselves may demand in negotiations additional security measures designed to protect employees, just as unions representing mail handlers have demanded personal protective gear now being provided to postal employees.

CHAPTER ENDNOTES

113 Much of the discussion of contract issues is taken directly from the original copyrighted *Checklist*.

114 The federal regulations governing pretreatment programs are found at 40 CFR Part 122 and 40 CFR Part 403.

Chapter 7

Insurance Against Terrorist Acts in the Wake of 9/11

Property and Casualty Insurance Against Terrorist Acts in the Wake of 9/11

The 9/11 attacks were the "largest single insured event in history."[115] Following the attacks, a massive number of insurance claims and cases were filed seeking recovery for losses suffered. See *e.g.*, *Parks Real Estate Purchasing Group v. St. Paul Fire and Marine Insurance Company*, 472 F.3d 33, 3 (S.D. N.Y. 2006).

Because some insurance policies excluded coverage for terrorist acts, Congress was moved to address the issue. The entire legal landscape of insurance for terrorist incidents has been changed due to the enactment of the Terrorism Risk Insurance Act of 2002, and its subsequent reauthorization and extension in 2005.

A. Insurance Coverage and Statutory Elimination of Terrorism Exclusions

The ultimate backstop for liability in the event of a terrorist attack is property and casualty insurance provided by the nation's insurance companies. While some water supply systems and wastewater treatment facilities are self-insured, and could rely upon their governmental immunity in such circumstances, many others purchase some form of casualty and property insurance from an insurance provider ("insurer"). Even those facilities that are otherwise self-insured may choose to seek coverage for terrorist attacks because the premiums for an individual facility are modest compared to the potential for massive property and casualty losses in the case of an attack.

After the 9/11 attacks, insurance coverage for terrorism largely disappeared.[116] Even if entities were able to obtain insurance coverage, it was nearly impossible to carry enough insurance to pay for all the potential damage. Congress passed the *Terrorism Risk Insurance Act*[117] (TRIA) in 2002 to help property and casualty policyholders obtain terrorism insurance from insurance providers. Such insurance is available for both public and private entities. TRIA renders void all terrorism exclusions in force on property and casualty policies of participating insurers— to the extent that such exclusions eliminate coverage for certified acts of terrorism as covered by the federal program.

Another important feature of TRIA is the ability of the insurer to recoup losses from the Treasury in the event that an act of terrorism exceeds certain statutorily mandated amounts per incident in insured losses. TRIA only covers acts of "terrorism" that produce property and casualty insurance losses in excess of $5 million (and otherwise fit the statutory definition). It leaves untouched the elements of other terrorism exclusions that deal with terrorist activity outside the scope of the federal program. For example, acts of domestic terrorism, such as the Oklahoma City bombing, or terrorism losses that do not reach the $5 million threshold are not covered.[118]

B. Federal Cause of Action for Torts Related to Terrorism

For negligence and tort law purposes, TRIA creates an exclusive federal cause of action for any property damages, personal injury, or death arising out of or resulting from an act of terrorism.[119] All state causes of action are preempted, and the federal action serves as the exclusive civil remedy for damages resulting from terrorist acts as defined under TRIA. TRIA provides, however, that the substantive tort law of the

state in which the terrorist act occurred is to be applied by the federal court in determining liability for damages for loss of life and commercial property. [120]

The only exception to the federal action are instances where an organization, government, or an individual knowingly participated in, conspired to commit, abetted, or committed any act of terrorism. Where such a finding has been made, the Act does not limit the liability of such a government, person or organization. If coverage under TRIA and other policies appears inadequate, individual water sector facilities may consider purchasing stand-alone terrorism insurance coverage. These stand-alone policies make no attempt to dovetail with the policyholder's property insurance coverage, which may contain various types of terrorism exclusions. Instead, these policies cover direct damage and, if endorsed appropriately, business interruption loss from a terrorist event, as defined in the policy. [121]

TRIA was originally set to expire on December 31, 2005. However, ten days before its expiration, President Bush signed the *Terrorism Risk Insurance Extension Act of 2005* into law, a reauthorization strongly supported by many public and private institutions. The legislation extends TRIA coverage until December 31, 2007. The Department of the Treasury has now promulgated regulations that implement TRIA as it was amended and extended in 2005. 30 C.F.R. Part 50. Congress is once again considering extension of TRIA during its current session.

Owners and operators of water sector facilities may consider reviewing their existing property/casualty, general liability and executive risk insurance policies and consult with their insurance brokers to ensure that the policy limits are adequate and that the scope of coverage is sufficiently broad to cover reasonably foreseeable property damage, personal injury and other claims in the event of a terrorist incident.

They also may consider obtaining current appraisals for their property and ensuring that the property is insured at its current value. Operators should pay particular attention to their business interruption insurance, including the amount of coverage and the length of the elimination period, to ensure they have sufficient coverage for foreseeable lost profits and extra expenses.

CHAPTER ENDNOTES

115 Jeff Woodward, "The ISO Terrorism Exclusions: Background and Analysis," IRMI Insights, Feb. 2002, available at: <http://www.irmi.com/Insights/Articles/2002/Woodward02.aspx>.

116 Id.; Jeffrey E. Thomas, "Exclusion of Terrorist-Related Harms from Insurance Coverage: Do the Costs Justify the Benefits?" 36 Indiana Law Review 397 (2003).

117 Pub. L. 107–297, 116 Stat. 2322, as amended, Pub. L. 109-144 (December 22, 2005), 15 U.S.C. § 6701 note. See generally ABS Consulting, Homeland Security Law Handbook, 2003, at Chapter 6.

118 See Jeff Woodward, "The Terrorism Risk Insurance Act of 2002," IRMI Insights, Dec. 2002.

119 Pub. L. 107-297 at § 107(a).

120 Id.

121 See Jack P. Gibson, "Terrorism Insurance Coverage for Commercial Property—A Status Report" IRMI Insights, June 2002.

CONCLUSION

The nation and indeed the world are confronting some of the most difficult challenges in human history. Much of the nation's infrastructure remains vulnerable to attack, yet protecting it from every conceivable threat is not only economically infeasible, but impossible. As the face of the terrorists, their origins, and their tactics evolve, so must society and its legal tools to combat terrorism. Our country, based upon fundamental principles of freedom and privacy, is navigating new territory in attempting to secure its infrastructure. Our citizens are being asked to make tradeoffs that are uncomfortable in a free society.

Because the attacks of September 11th have forever changed life in the United States, it is important to prepare for the unexpected by utilizing and understanding the role of vulnerability assessments, corrective actions, emergency planning, and the control of security information. Since 9/11, the United States has experienced an unprecedented expansion of governmental entities and legal frameworks designed to address terrorist threats. It is essential to study other industries dealing with the same new territory and to consider all that they have learned since September 11, 2001. Ultimately, worldwide cooperation will be essential to a secure future. This publication, together with tools provided by APWA, AMWA, NACWA, WEF and others, are intended to assist water sector facilities in dealing with the wide range of legal and policy issues springing from the possibility of such attacks, but not yet fully known or comprehended.

A CHECKLIST FOR OWNERS AND OPERATORS

THE NATURE OF TERRORIST THREATS TO WATER SECTOR INFRASTRUCTURE 4

___ What generic types of security threats does the water sector face

___ What are the health, safety, and the environmental implications of an attack on the water sector

___ What are the consequences for the nation of an attack on the water sector

THE FEDERAL LEGISLATIVE FRAMEWORK FOR PROTECTING WATER SECTOR INFRASTRUCTURE 8

___ What are the legal, policy, and practical responses to terrorist threats

___ How have the legal and policy security requirements for the water sector evolved since 9/11

___ What are the roles of the Department of Homeland Security and the U.S. Environmental Protection Agency in leading the water sector response to terrorist threats

___ The federal government's Water Sector plan and framework for response to terrorists threats: The Critical Infrastructure and Key Resources Water Sector-Specific Plan as Input to the National Infrastructure Protection Plan

THE SAFE DRINKING WATER ACT MODEL FOR MANDATORY VULNERABILITY ASSESSMENT PREPARED BY WATER SUPPLIERS 8

___ SDWA requirements for a vulnerability assessments for water suppliers

___ What are the legal implications of failure to take corrective actions in response to a vulnerability study

___ SDWA protections against disclosure of vulnerability studies

VULNERABILITY ASSESSMENTS FOR WASTEWATER FACILITIES 10

___ What is the current status of federal legislative efforts regarding vulnerability assessments for wastewater treatment facilities

___ State and local requirements pertaining to vulnerability studies

___ Considerations if undertaking a voluntary vulnerability assessment

___ Obligations created by undertaking a vulnerability assessment

___ Access by members of the public or press to the vulnerability assessment and underlying documentation

___ Providing vulnerability assessments to the state and/or federal government

___ Maintaining confidentiality of a vulnerability assessment

___ Prospects for future legislation to address the confidentiality of vulnerability assessment

THE DUTY TO PROTECT THE PUBLIC FROM KNOWN OR FORESEEABLE TERRORIST ATTACKS AND THE POTENTIAL CIVIL LIABILITY FOR CONSEQUENCES OF TERRORIST ACTS 16

___ What are the tort principles of due care and how are the standards of negligence law applied to water sector owners, operators and facilities

___ The developing common law on failure to secure facilities from terrorist attack

___ The first tort case to address failure to secure a facility from a terrorist attack: The 1993 World Trade Center Bombing Case

___ The continuing World Trade Center litigation following the attacks of 9/11, and the emerging law of negligence in the context of terrorist attacks

___ What are the other potential common law liabilities for failure to secure against terrorist attacks

___ What potential statutory defenses exist to a negligence suit based upon failure to adequately protect a water sector facility from terrorist attacks

___ Does strict liability for ultra-hazardous activity exist for water sector vulnerabilities to terrorist attacks

___ Recent cases involving governmental immunity in civil liability actions following terrorist attacks and their applicability to publicly owned water supplies and treatment works

___ Effect of governmental warnings of credible threats on liability

___ Effect of public information regarding possible threats on liability

___ Effect of a declaration of war on obligations, duties, and operations

___ Causes of action under federal environmental law for a release of hazardous materials or substances related to terrorism or vandalism

___ State laws allowing claims for exposure and damages to environmental releases

___ Causes of action at common law for a release of hazardous materials or substances related to terrorism or vandalism

PARTICULARIZED DUTY TO EMPLOYEES REGARDING TERRORIST THREATS AND ATTACKS.....26

___ The World Trade Center Disaster Site Litigation and the rights of first responders and other employees at facilities attacked by terrorists

___ Worker compensation laws: exclusive remedy for certain class of workers following terrorist attacks

___ Applicability of *The Occupational Safety and Health Act* and State Workplace Safety Statues to workplaces in general and the water sector in specific

___ Employee civil rights and making employment decisions free of bias related to race, religion, national origin and ethnicity

___ Employer response to potential health impacts to employees from terrorist acts or threats of terrorism

___ *Americans with Disabilities Act* compliance following a terrorist attack

___ Preventing employee harassment or workplace violence as a result of bias triggered by terrorist attacks

___ General duties to provide a safe workplace

___ Testing the workplace environment for biological threats

___ Responding to employee requests based upon fears of risk in the workplace

___ Employee insurance, medical leave, and related policies

___ Obligations to employees accused of criminal activity

MANAGING INFORMATION WITH THE POTENTIAL TO IMPACT THE SECURITY OF WATER SECTOR INFRASTRUCTURE.....36

___ Understanding the delicate balance between the need to keep information from terrorists and the government's and public's right to know

___ Legal tools for preventing the unauthorized disclosure of water infrastructure security information that would directly aid terrorists

___ The evolution of statutory protection for vulnerability assessments

___ Access to vulnerability assessments and other security information prepared by water suppliers

___ Access to vulnerability assessments and other security information prepared by wastewater treatment facilities

___ The *Freedom of Information Act* exemptions from disclosure and state statutory protections under state freedom of information laws

___ Other state statutory and common protections

___ Required disclosure of vulnerability assessments to the government

___ Preventing access to water sector facilities designs, plans, and specifications

___ Facilitating the dissemination of security information to thwart terrorism

___ Ongoing and future research needs to improve systems to thwart terrorism

___ The critical role of the Water Information Sharing and Analysis Center (WaterISAC) in the dissemination of information to thwart terrorism in the water sector

___ The critical role of the Water-Wastewater Agency Response Networks (WARN) in thwarting terrorist acts in the water sector

OBTAINING SENSITIVE EMPLOYEE INFORMATION IN AN EFFORT TO PREVENT ACTS OF TERRORISM 46

___ Employee civil rights relative to collection of sensitive information

___ Screening of new employee applicants to prevent terrorist infiltration

___ Background checks on existing employees and employee rights

___ Excluding potential water sector employees based on criminal records

___ Handling of immigration violations identified during background checks or employee screening

___ Restrictions on the surveillance of employees in the workplace

___ Communication of new surveillance measures to employees

___ Union contracts and their impact upon employee screening

___ Impact of new federal laws on surveillance and cooperation with federal investigation authorities: *The USA Patriot Act*

___ Monitoring employee records and activities at the workplace

___ Communication of new measures to maintain workplace security

___ Monitoring employee health or requesting employee health exams

___ Handling governmental authority requests to interview or investigate employees

LIABILITY FOR RELEASES OF HAZARDOUS MATERIALS AS A RESULT OF AN ACT OF TERRORISM OR VANDALISM 56

___ The requirement to report releases

___ Substantive federal environmental law causes of action applicable to a release of hazardous materials or substances as a result of an act of terrorism or vandalism

___ Potential liability under CERCLA (Superfund)

___ Potential *Clean Water Act* liability

___ Potential *Clean Air Act* liability

___ Substantive state causes of action for release of hazardous substances as a result of a terrorist attack

___ Potential liability under state environmental statutes

___ Potential liability under state common law principles

___ Negligence

___ Trespass

___ Public and private nuisance

___ Reporting requirements in the event of a release

CONTRACT ISSUES 66

___ Contracting with Third Parties

___ Union Contracts

___ Contracts with outside service providers

___ Suppliers and vendors of materials

___ Reopening existing contracts

___ Addressing crisis events in new contracts or contract renewals

___ Verifying contract customers are complying with legal requirements relating to security

___ Rights of entry to monitor customers' compliance with security requirements

___ Contract termination for security concerns

___ Effect of existing union contracts

___ Effect of crisis events on future negotiation of labor contracts

INSURANCE AGAINST TERRORIST ACTS IN THE WAKE OF 9/11.....70

___ Insurance coverage and statutory elimination of terrorism policy exclusions: the *Terrorism Risk Insurance Act*

___ Federal cause of action for torts related to terrorism

___ Determining whether there is adequate coverage for property damage, death or disability that results from an act of terrorism or crisis event

___ Exclusions from coverage in existing insurance policies

___ Changes in insurance policies following an act of terrorism or crisis event

___ Possible coverage for otherwise "self-insured" governmental entities in the water sector

American Public Works Association
Washington DC Office
1401 K Street, NW, 11th Floor
Washington, DC 20005
202.408.9541

Headquarters
2345 Grand Boulevard, Suite 700
Kansas City, MO 64108-2625
816.472.6100
800.848.APWA
www.apwa.net

Association of Metropolitan Water Agencies
1620 I Street, NW
Suite 500
Washington, DC 20006
202.331.2820
www.amwa.net

National Association of Clean Water Agencies
1816 Jefferson Place, NW
Washington, DC 20036-2505
202.833.2672
www.nacwa.org

Water Environment Federation
601 Wythe Street
Alexandria, VA 22314-1994
703.684.2400
http://www.wef.org

In association with:

Dewey & LeBoeuf
1101 New York Avenue, NW
Suite 1100
Washington, DC 20005
202.986.8000
www.deweyleboeuf.com