USAWC STRATEGY RESEARCH PROJECT

ANALYSIS OF U.S. WATER INFRASTRUCTURE FROM A SECURITY PERSPECTIVE

by

Colonel Paul L. Grosskruger
United States Army

Richard Meinhart, Ed.D
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
15 MAR 2006		**00-00-2005 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Analysis of the U.S. Water Infrastructure from a Security Perspective	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Paul Grosskruger	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**24**	

ABSTRACT

AUTHOR: Colonel Paul L. Grosskruger

TITLE: Analysis of U.S. Water Infrastructure from a Security Perspective

FORMAT: Strategy Research Project

DATE: 15 March 2006 WORD COUNT: 6,217 PAGES: 23

KEY TERMS: Terrorism, Interagency

CLASSIFICATION: Unclassified

The U.S. National Security Strategy for Homeland Security identifies the U.S. water infrastructure as one of the nation's critical infrastructures. Experts and several reports to Congress point out the vulnerabilities of domestic water supply and distribution systems to terrorism and the ramifications of a successful attack. Starting in the late 1990s, the federal government implemented a host of actions intended to protect domestic water supplies. Despite these efforts, critical vulnerabilities remain within the water infrastructure, especially in understanding threat vulnerabilities, in developing long-term federal funding strategies, in appropriate information-sharing, and in incorporating technologies. This paper analyzes the nation's water infrastructure, reviews relevant threat vulnerabilities, and explores needed responses by federal, state, and local governments and private industry authorities. This paper identifies open strategic issues needing immediate attention and provides recommendations for a unified, comprehensive strategy to address the security concerns within the U.S. water infrastructure.

ANALYSIS OF U.S. WATER INFRASTRUCTURE FROM A SECURITY PERSPECTIVE

Events of September 11th, 2001 serve as a grim reminder of how dangerous our world has become as the nation awoke to the harsh reality that it wasn't secure within its own borders. This cataclysmic event caused the U.S. government to reevaluate its domestic security posture and take necessary actions to protect the nation from terrorism. To meet this new challenge, the Bush Administration and those that follow must strive to understand the nature of this threat and devise effective security strategies to protect the nation's people and infrastructure. Not long after the 9/11 tragedy, President Bush reflected on this challenge and set clear priorities emphasized in his 2002 *U.S. National Security Strategy for Homeland Security*: "There is a strong consensus that protecting the people from terrorist attacks…is among the highest, if not the highest, priority any government can have."[1] The President has made homeland defense a resonating theme in all his security strategies. For example, his 2002 *National Security Strategy,* the capstone document for all federal security strategies, emphasized, "Defending our Nation against its enemies is the first and fundamental commitment of the Federal Government."[2] It is clear that the U.S. government must take new approaches to protect its population and its infrastructure from any future terrorist threats to the homeland.

Today's terrorism takes many forms. While many think of bombs going off in a crowded street or other methods of violence, what if the threat was as close as the water tap? As the Department of Homeland Security's *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* points out: "The basic human need for water and the concern for maintaining safe water supply are driving factors for water infrastructure protection."[3] While some may say the threat to water is unlikely, attacks on water sources are nothing new and have been a common tactic since ancient times.[4] In fact, a 1998 report urged more interest and funding for water security: "Obviously, there are costs associated with hardening water supply systems. The costs of [water] system hardening can be viewed as analogous to paying for means of countering potential terrorist threats against the airline industry."[5] H. Court Young, a respected author and expert on the subject of water and terrorism, also asserts the importance of addressing water terrorism by observing that the federal government has acknowledged that the nation's water supply, due to its "extensive infrastructure [has been] vulnerable to terrorist attack since the 1990's."[6]

Since many experts see water terrorism as a possibility within the United States, our nation's leadership must address the following three key questions: How safe is our water supply today? Do we fully understand the water infrastructure's vulnerabilities? And what must

the federal government do to ensure the protection of this critical infrastructure? Previous work by water infrastructure experts, government reports and other studies indicate that despite efforts at all levels, these questions are not fully answered. Many indicators point to the need for the federal government to take a more assertive role in examining the effectiveness of the actions over the past four years and make a more concerted effort in tackling issues such as: clearer lines of authority and leadership in integrating security actions; a comprehensive funding strategy; clearer monitoring standards; and promotion of more collaborative approaches across the national infrastructure. EPA's Acting Secretary for Water, Benjamin H. Grumbles, summarized the situation in his 2004 testimony to Congress: "We have good news to report on our progress to date. However, much work remains to be done…"[7]

In examining the threat to the U.S. water infrastructure and identifying needed security actions, this paper explains the nature of the threat and the water infrastructure system. It first reviews historical examples of water terrorism and its strategic consequences. To clearly understand strategic vulnerabilities, it summarizes the major components of the U.S. water infrastructure, providing the reader an appreciation of the diversity, complexity, and breadth of the infrastructure thereby honing into the areas most vulnerable. After this review, the paper explores the intent and water security actions of the federal government, lead governmental agencies, state local government and by private industry. This provides a review of both accomplishments and policy gaps needing attention. The paper concludes with recommendations to senior governmental officials and organizations on the next steps necessary to better achieve national water infrastructure security.

Understanding the Threat to Water

A study of history affirms that an attack on an enemy's water supply is surely plausible. Rooted in ancient times, this form of asymmetric warfare remains relevant today. Hickman observes in a 1999 Air War College research paper that adversaries have viewed water as a center of gravity and an Achilles Heel.[8] He points out several examples of armies from the ancient Romans, through the Civil War, and World War II that have used toxins such as cyanide, cholera, anthrax, or animal cadavers to poison water supplies and deny the enemy this critical resource. He correctly warns that the United States must prepare for water terrorism in this day and age, as future U.S. adversaries will likely use it to achieve their strategic objectives.

Historical examples reinforce recent intelligence reports on Al Qaeda's intent to target the U.S. water infrastructure. In 2002, the FBI reported that a computer was seized by U.S. authorities in Afghanistan containing technical information on U.S. water infrastructure and

sophisticated engineering design software.[9] Additionally, the FBI found indicators that Al Qaeda had attempted to hack into U.S. water infrastructure control systems, and the FBI's National Infrastructure Protection Center issued a bulletin indicating it believed members of al Qaeda were attempting to hack into the remote control systems of water treatment facilities.[10] This affirms Al Qaeda's interest in both the infrastructure and its vulnerabilities. Jeff Stone summarizes this vulnerability in his article *Minimizing Security Risks of Public Water*: "A water system is an attractive target to a terrorist.…The potential for causing panic among the public is great due to the essential nature of safe drinking water and the public's trust in their drinking water systems."[11]

Despite the apparent threat, the likelihood of a successful terrorist attack on the nation's overall water system can be considered low. Many experts claim there is little to no threat to the source water due to the enormous dilution factor. Additionally, treatment processes prior to water's entry into the distribution system, security measures, observation, and periodic monitoring could deter terrorists. A recent American Water Works Association report stated: "Most water systems have so much water and such effective treatment mechanisms, that anything less than many tankers full of dangerous agents would be diluted and easily neutralized."[12] A recent study on bioterrorism attacks on water supplies stated: "targeting large bodies of water would be impractical."[13] Secondly, any input at this point would most likely be detected and treated by conventional treatment processes once it reached the treatment facility. Simple chemical processes and disinfection would eliminate biological hazards prior to discharging these hazards into the water distribution systems.

While the risks to source and treatment components of the water infrastructure are low, several experts do agree that the water distribution component is vulnerable. Within this component, terrorists have the highest probability for executing a successful attack due to ease of access and amounts of contaminants required to cause illness or death—or to simply cause widespread panic. Since terrorists may identify water distribution as a lucrative option, they could introduce a chemical or biological agent into the system or remotely hack into a municipality's control system. While many types of industrial chemicals can do the job, a more sophisticated approach is introducing weaponized biotoxins.[14] A potential terrorist could remotely hack into control systems and shut down water supplies to major cities or shut down waste water systems thereby causing major health and environmental hazards. Even a limited attack could have far-ranging strategic impacts.

Water Contamination Examples

Given the nature of 21st Century terrorism and its multidimensional threat to the U.S. population, two compelling contamination examples occurred within the past 20 years that can provide valuable insights to U.S. policymakers. The first example deals with a case of accidental contamination in the city of Milwaukee, Wisconsin in 1993. In this case, a dangerous organism found in mammal feces, Cryptosporidium, "passed undetected through two water treatment plants and, once it reached customers' taps, caused more than 400,000 illnesses (mostly diarrhea) and between 50 and 100 deaths out of some 800,000 customers who drank the water."[15] This situation caused widespread panic as the population and local governments grappled with the appropriate response.

A second situation was a November 1985 incident at the U.S. Military Academy in West Point, New York. Apparently an unidentified caller claimed that the Academy's water supply had been sabotaged. After extensive sampling and testing, the plant operators could not find any contamination. Despite this fact, Academy officials refused to allow the plant to operate until all testing was verified. The impact to the Army Post caused panic and disruption of the installation's operations and "the issue of water deprivation was a critical concern."[16]

The Milwaukee incident highlights the broad potential for illness, death, and panic within the population and confusion by local authorities. Likewise, the incident at West Point demonstrates the psychological effects of a perceived threat to a local water supply. Perhaps the most important lesson drawn from these two cases is that any successful strategy to secure water must address the following: a means to continuously monitor water quality and pinpoint suspected attacks within the system; a plan that educates and reassures the public; and a means to rapidly respond to suspected attacks. These important lessons—along with a clear understanding of the components and vulnerabilities of the water infrastructure—provide the necessary underpinnings of a successful water infrastructure security strategy.

Understanding the Domestic Water Infrastructure

To better understand water supply security issues, this paper will now take a macro-level look at the various components of the water infrastructure. With this overview, policymakers with a limited technical background can visualize interdependencies within the system, focus on potential vulnerabilities, and devise the best strategies to reduce the threat. There are approximately 168,000 public water systems within the United States. These systems range greatly in size, serving from as few as 25 persons to more than 1 million persons.[17] For example, "Of the approximate 168,000 water systems, 53,363 water systems are considered

community water systems that serve a residential population of nearly 270 million year-around, approximately 90 percent of the population."[18] An important point discussed later is that of the 53,363 systems, 15 percent serve populations of 3,300 or more people.[19] Clearly, the complex, varied, and expansive nature of the water infrastructure poses challenges for the strategic policymaker.

This diverse water infrastructure can be further broken down into discrete components, which then enable policymakers to identify and understand potential vulnerabilities. Each water supply system, regardless of its size, consists essentially of three major components: the source of raw water and its transport to the treatment process; the treatment and distribution system for treated water; and the transport, treatment, and discharge of waste water.[20]

The first major component, the source water system and conveyance to the treatment process, consists of reservoirs, lakes, rivers, streams, and wells which connect to the intakes of conveyance systems and treatment facilities. Large reservoirs operated by the Bureau of Reclamation are particularly important for providing water to the western United States.[21] The U.S. Army Corps of Engineers also plays a key role in managing water resources by providing water to thousands of cities and industries from 9.5 million acre-feet of water stored in 116 lakes and reservoirs across the country.[22] Of the three parts of the water infrastructure, the source water system is the easiest to attack. Yet attacks on the source, as discussed earlier, pose the least risk to the population. A 2004 U.S. Army Engineer Research And Development Center (ERDC) report further stated: "The amount of contaminant required to permeate the whole [source water] system would, after taking dilution into account, either be too large to handle…or far more expensive than other terrorist weapons."[23] This fact shouldn't rule out the possibility of a terrorist attack, but rather it should influence strategic policymakers into focusing finite resources toward other more vulnerable components of the water infrastructure.

The second major component of the water infrastructure is the water treatment system. This component is very diverse, consisting of literally thousands of various public and private water systems and utilities. To complicate things further, water utility staffs vary in size and capability as facilities and treatment processes vary. In this component, the source water is conveyed to the water treatment plant and treated to meet standards for drinking and other uses. This water treatment component consists of physical and chemical treatment processes including sedimentation, filtration, and chemical additions to meet standards. W.D. Burrows, a clinical water expert at the U.S. Army Center for Health Promotion and Preventive Medicine, points out that water treatment processes will remove most biological pathogens, biological agents, and bio-toxins but some could pass through. Hence, he recommends a need for a

continuous monitoring method for biological agents and other security measures within the water treatment process.[24] In *Understanding Water and Terrorism,* Young warns that within the treatment process, the primary vulnerability is access to various injection points. He states: "Large metropolitan water systems generally have multiple points at which they inject chlorine into the water supply. Water from the clearwell goes directly into the distribution system. This makes clearwells a critical point for any terrorist attempt."[25] The security focus within this component is essentially twofold: denying unauthorized access into the system; and real-time water quality monitoring to ensure safe drinking standards.

Once conventional treatment is complete, water passes into the third component—the distribution system—which experts appear to agree is most vulnerable to terrorist attack. This component is divided into two parts: the water distribution system and the wastewater treatment and discharge system. The water distribution system consists of storage tanks, miles of pressurized water pipes, and an intricate distribution system that ultimately leads to the home tap. The previously cited ERDC study sends clear warnings on potential vulnerabilities within the distribution system. More recent studies by the Corps of Engineers, along with others, claim the following: chemical/biological attacks could be carried out for as little as 80 cents per lethal dose; a single individual can obtain or produce effective contaminants in quantity; and contaminants can be introduced into the distribution system without the aid of pumping equipment via a method called backflow attack.[26] In addition to actual harm, there is the potential psychological impact of a terrorist attack, and the ERDC warns of 2d and 3d order effects of such an attack. A utility's first response of simply turning off the water flow could cause significant long-term problems such as "pipe implosion and various forms of valve and pump loss,"[27] which then effectively negates water delivery for days or weeks.

The waste water treatment and discharge system consists of miles of sewer pipe, lift stations to the waste water treatment plant, and the discharge system. This sub-component is highly regulated by both state and federal agencies, since it discharges water back into the nation's rivers, streams and aquifers. A significant threat to the waste water system would be an interruption of power, thereby causing treatment and discharge systems to release massive amounts of untreated water back into the ecosystem. This threat could come from a cyber attack, where electrical systems connected to the water plant are accessed remotely and shut down. Another technique would be an attack on critical pump stations which could cause a half million people to lose their water instantly, and since pumps are often custom-built, the utility would be out of commission for months or over a year.[28]

The water infrastructure's diverse nature suggests that the answer to these challenges just discussed should be equally diverse—that is, a decentralized, "bottoms-up" approach, which leverages the expertise and concerns of local and regional municipalities coupled with a responsive "top-down" approach led by the federal government. The "top-down" responses by the federal government will now be examined.

Federal Government Actions, Policies and Strategies to Address Water Terrorism

The Federal government recognized the threat to the nation's water infrastructure over the past decade and made significant strides in addressing concerns. In the 1990's, the Clinton Administration, through Presidential Decision Directive (PDD) 63, identified the water supply as a critical infrastructure and tasked the Environmental Protection Agency as the lead federal agency to plan and coordinate efforts. Additionally, this directive identified requirements for interagency cooperation, vulnerability assessment, research and development, intelligence sharing and international cooperation.[29] While this directive gave guidance to federal agencies, it lacked enforcement since it held no regulatory authority over the water infrastructure and provided no funding to back it up. Despite this directive and several warnings by academia and private industry, strategic efforts to address water terrorism essentially remained dormant until after September 11th, 2001.

After 9/11, both the Bush Administration and Congress set in motion homeland security strategies, policies, and legislation that brought sweeping changes to the Federal government to protect the population, its key assets, and its infrastructure—including water. The Administration enacted the most significant reorganization of the Federal government since the 1950's with the establishment of a Department of Homeland Security. The Department of Homeland Security combined 22 federal departments and agencies, introduced a *National Strategy for Homeland Security,* and identified strategic objectives, critical mission areas, and roles and responsibilities of government and private industry. Since 2002, the Department of Homeland Security (DHS) has been the agency responsible for meeting the challenge of developing strategic policy, coordination, and response for protecting the nation's infrastructure.

The underpinning principles of the *National Strategy for Homeland Security* (NSHS) are based upon mutual cooperation of all levels of government and private industry representing over 87,000 water jurisdictions across the nation. The NSHS emphasizes this critical reliance: "State and local governments have critical roles….The private sector—the Nation's principal provider of goods and services and owner of 85 percent of our infrastructure—is a key homeland security partner."[30] Additionally, the NSHS provides general direction with respect to

allocation of federal funds, cost sharing, setting national security priorities, and critical mission areas.

To reduce vulnerabilities to terrorist attacks, the NSHS identifies six critical mission areas within the overarching strategy. One of the mission areas, protection of critical infrastructures, addresses water infrastructure protection as one of the 13 critical infrastructure sectors. The Environmental Protection Agency (EPA) is designated as the lead federal agency for addressing water security matters and other federal agencies have supporting roles. In addition to providing an overarching strategy, the NSHS called for a "comprehensive national plan to protect America's infrastructure from terrorist attack,"[31] later known to be the *National Response Plan* and the development of *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets,* published in February 2003.

The strategic objectives and responsibilities of all levels of government and private sector in the nation's water infrastructure are specified in both plans. The *National Strategy for Physical Protection of Critical Infrastructures and Key Assets* identifies three strategic objectives in protecting the nation's infrastructure: identify and assure protection of critical infrastructure; provide timely warning; and enable a collaborative environment between state, federal, local and private sectors.[32] The strategy also outlines general guidance on the concept of shared responsibility among state, federal, local and private entities. It also highlights eight guiding principles that include: assuring public safety and confidence, establishing responsibility and accountability, facilitating partnering and developing market solutions, and harnessing technologies in addressing the terrorist threat.[33]

The *National Response Plan* offers detailed guidance for responses to both natural disasters and acts of terrorism within the United States. The plan specifies responsibilities, roles and planning required by federal, state, local governments and private entities. Regarding threats to the nation's water supply, the *National Response Plan* mandates a host of interagency planning and response actions. An attack or perceived attack on the water supply would trigger the Interagency Incident Management Group (IIMG), led by DHS and composed of all federal departments and agencies, to coordinate the national response.[34] Other organizations cited in the plan include the Homeland Security Operations Center (HSOC), an ad hoc group formed immediately after an incident to work operational matters and maintain situational awareness that also coordinates across the entire infrastructure.

As a complement to the *National Response Plan*, the *Federal Response Plan* (FRP) provides: "The mechanism for federal departments and agencies to coordinate delivery of Federal assistance… [namely] for a major disaster or emergency, including terrorist acts."[35] In

the event of an attack on any component of the water infrastructure, the FRP designates the Department of Justice (DOJ) as lead federal agency, which then normally delegates on-site actions on investigation and other law enforcement actions to the Federal Bureau of Investigation (FBI). Other agencies assisting in response would be the DHS, the Federal Emergency Management Agency (FEMA), the Department of Health and Human Services (HHS), the Department of Defense, and the Environmental Protection Agency. The EPA's role in an actual response would mostly involve technical support and advice on remediation matters. The Department of Defense's U.S. Army Corps of Engineers (USACE) serves a major role in supporting the water infrastructure by providing emergency restoration of critical facilities, temporary restoration of critical water supplies, and emergency contracting.[36]

The executive branch has clearly developed strategies and plans, but perhaps the most far-reaching action toward protecting the nation's water supply has come from Congress. After the 9/11 terrorist attacks, Congress held a series of hearings on water infrastructure security which identified vulnerabilities of the water infrastructure to terrorist attacks and provided exceptional insights to address this national challenge.[37] This testimony and other Congressional research studies into the matter set into motion sweeping legislation on water security. As a result of these hearings, on 12 June, 2002 President Bush signed Public Law 107-188*,* the *Public Health Security and Bioterrorism Preparedness and Response Act of 2002.* The Act attempted to secure the water infrastructure by identifying responsibility, setting requirements to achieve water security, and providing initial funding.

The *Bioterrorism Preparedness and Response Act of 2002*, actually an amendment of the *Safe Drinking Water Act,* is currently the legislative cornerstone of the water infrastructure's defense against terrorism. This Act's intent, as pointed out in the *National Response Plan*, is to "improve the ability of the United States to prevent, prepare for and respond to bioterrorism and other public emergencies."[38] This Act requires community water supplies (CWS) serving populations of 3,300—over 90 percent of the U.S. population—to develop vulnerability assessments and emergency response plans. For smaller community needs, the Act requires the EPA to provide guidance on vulnerabilities and emergency planning to support them. The Act also requires the EPA to collect and certify all water infrastructure vulnerability assessments and explore methods of addressing terrorist attacks using means such as: developing real-time monitoring methods; education and awareness programs; developing technologies and equipment upgrades to prevent the flow of contamination into drinking water systems; and researching ways to mitigate effects on public health. It also stipulates that the EPA would take lead responsibility in information-sharing by means of the Information Sharing and Analysis

Center (ISAC). It also requires the EPA to develop a "strategic plan that addresses methods and means by which terrorists…could disrupt…drinking water"[39] and provides funding for programs and research supporting the security of the nation's water supply.

Analysis of Federal Actions

While actions by the executive branch and Congress produced improvements in security, research indicates that four overarching deficiencies remain within the current strategy: confusion in federal agency roles and responsibilities; poor linkage between infrastructure vulnerability assessments and federal funding; lack of measurable performance standards; and lack of authority in enforcing security standards. Each of these deficiencies will now be examined followed by recommendations to address these deficiencies and improve security of this critical infrastructure

Clarifying Federal Agency Roles and Responsibilities.

After review of the *Bioterrorism Preparedness and Response Act*, the *National Response Plan* and the *Federal Response Plan*, it is difficult to understand who is actually in charge. With respect to confusing roles and responsibilities, Mary Tiemann's cites in a recent report that: "Congress has expressed concern that, overall, EPA's homeland security responsibilities have not been well articulated."[40] As discussed earlier, federal plans assign authority to various federal agencies and fails to place the lead integrating agency, the Department of Homeland Security, squarely responsible for integrating security actions.

Tiemann recommends that the Department of Homeland Security and Environmental Protection start to clarify the confusion through a Memorandum of Understanding (MOU). This is only a partial solution. The confusion on who's in charge reinforces current concerns of the effectiveness of interagency response in times of emergency. Certainly roles tend to sort out with time, but we really do not have this kind of time. Increasing the risk is the fact that there is little to no precedent on federal response to water terrorism. This research indicates that the answer to these roles and responsibilities problems lie with legislation and a federal strategy that clearly delineates federal roles in the planning and response to attacks to the water infrastructure. Hence, the Department of Homeland Security should take a more assertive role in integrating water infrastructure security efforts. The DHS is in the best position to integrate security efforts ranging from threat analysis and prioritization of federal response efforts to sharing information and presenting recommendations to the executive and legislative branches.

Linking Infrastructure Vulnerabilities to Federal Funding

The EPA has the major mission of translating both the 2002 Act and other national strategies into comprehensive, feasible, and effective security plans—easier said than done. Although the EPA has done some preliminary work toward understanding the vulnerabilities of the nation's water infrastructure, a 2003 Environmental Protection Agency Inspector General's report pointed out key issues involved with its implementation. The Inspector General found in interviews with several water utility officials that the vulnerability assessments do not adequately address terrorist threats and were geared more toward traditional and less costly threats such as vandalism and disgruntled employees.[41] The report found that neither the Bioterrorism Act nor the EPA provided water utilities with detailed guidance on the minimum terrorist threat to address in their vulnerability assessments. This is a significant finding, that the EPA, "made no effort to provide credible threat information" and directed vulnerability assessments be done based upon the subjective judgments of what the utility community defined as a threat. This is a costly misstep, since the federal government will direct finite funding largely based upon these vulnerability assessments.

While the 2002 Bio-Terrorism Act provided, for the first time, some funding toward protecting the water infrastructure, the issue of resource allocation has yet to be fully resolved. As pointed out in congressional testimony: "Many water systems that have completed their vulnerability assessments are now saying, 'we have identified our weaknesses, now what do we do?'"[42] This issue was examined in a 2003 General Accounting Office Report that pointed out issues with funding prioritization. It concluded that utilities serving the largest population densities should receive priority, followed by other sensitive utilities such as military installations, universities and cultural sites.[43] This conclusion may create a contradiction, since the same report pointed out that the utilities' vulnerability assessments should also be strongly considered in prioritization. The EPA, therefore, is faced with making case-by-case judgment calls on the proper allocation of Federal funding.

The solution to the problem of linking vulnerabilities with federal funding strategies resides at a level above the EPA. The EPA, by its very nature, is incapable of effectively translating national security policy objectives into applicable security requirements across this broad and diverse infrastructure. The federal agency needed to take the lead role in infrastructure security strategy formulation, development of funding strategies, and lead in federal response is the Department of Homeland Security. Hence, this paper recommends that the DHS assert its position as the lead agency in domestic security and, by using expertise across all federal agencies and collaborative approaches with regional and local municipalities, develop a holistic

infrastructure vulnerability assessment. This DHS's leadship through both a "top down" transmission of vulnerability information combined with fostering a "bottoms up" collaborative approach gives both the President and Congress one point of contact in infrastructure security matters.

Monitoring Standards for the Water Infrastructure.

A key issue directly in the EPA's court centers upon the need for specific water quality indicators and measurable performance standards to reduce risks to the water infrastructure and the population. As identified in a 2003 EPA Inspector General Report, the EPA has not issued standards to the water infrastructure and has not obtained or analyzed data to develop a baseline for water security.[44] This is a critical step. Without established standards and benchmarks, the water industry and the government have no idea on what exactly constitutes a vulnerability. Instead of developing standards, the report pointed out that the EPA simply focused on complying with the 2002 Bioterrorism Act, which required completing vulnerability assessments. Baseline standards provide valuable information to the water infrastructure and serve a basis for any real-time monitoring and warning system in the water supply. In addition, collection of data also provides the federal government with an overall assessment of vulnerabilities in the water infrastructure.

To respond to this problem, this paper recommends a concerted effort be taken between the EPA, academia, and industry in identifying indicators of water tampering coupled with baseline water monitoring standards aimed at detecting these contaminants. Additionally, they need to embrace rapid monitoring technologies that constantly verify these water quality standards to significantly reduce the impact to both the utility and the public. By aggressively using today's technological breakthroughs in monitoring and data transmission coupled with clear baseline standards, the federal government could address this gap immediately.

Enforcement of Security Standards.

Some experts are concerned that the Bioterrorism Act falls short in providing the EPA the authority to enforce standards in water security. In a Georgetown Law Journal, Varu Chilakamarri argues that the Act may have stretched the EPA too far in its ability to enforce its intent when he stated: "In assigning the EPA the mission of securing the public water supply from terrorism…Congress left…several flaws that could render the whole effort futile."[45] Chilakamarri recommends more authority be given to EPA to stringently enforce requirements, which remains an open issue. The EPA has proceeded forward with a heavy emphasis on issuing the water infrastructure guidance, developing systems for information sharing, and

partnering approaches vice a heavy handed approach. This current approach lends to an uneven application of security measures across the nation and produces open security gaps.

To solve this problem, a more stringent approach is likely needed to ensure water security, as we currently do with water quality. Four years have passed since the 2002 Bioterrorism Act, and the federal government is now in a position to codify uniform baseline security standards and back these standards up with appropriate enforcement measures. This paper recommends that such security standards be tied directly to adequate funding across the infrastructure to meet security standards. Within federal legislation and policy, EPA should be designated as lead in monitoring standards and enforcement.

State, Local and Private Water Infrastructure Actions on Water Security

While the federal government addresses gaps in national policy, the regional, local and private entities are in the best position to identify and address local security needs. Efforts in Florida by state agencies, local municipalities, and private utilities serve as an example of an effective "bottoms up" approach in addressing water security. Florida's initiative provides a cost-effective approach in information sharing, developing vulnerability assessments, collaborating in emergency response planning and execution, and addressing public health issues. A closer examination of initiatives in Florida may provide the final piece of the puzzle needed to better secure our nation's water infrastructure from terrorism.

According to a report by the Florida Department of Environmental Protection (FDEP) and the Florida Department of Health (FDOH), 12 million Floridians and 40 million annual visitors are served by large water systems. The FDEP and FDOH have established strong state interagency partnerships that deal with water quality, emergency response planning, counter-terrorism, and public health issues. Both agencies, which coordinate closely with federal agencies, have established a coalition to address the terrorist threat consisting of four working groups: Emergency Response; Drinking Water Safety; Laboratory Coordination; and Communications. [46]

Florida possesses a wealth of expertise in dealing with natural disasters, and its work in this area links closely with addressing the challenge of domestic terrorism. Through a combination of experience and innovation, Florida has formed effective partnerships reaching across all levels of government and throughout the private sector. One such partnership that is a model for addressing natural and deliberate threats is Florida's Water-Wastewater Agency Response Network (FlaWARN). This coalition defines itself as "a formalized system of utilities helping utilities to address mutual aid during emergencies"[47] and is based upon a voluntary

arrangement between state and local government agencies, academia, and regional public utilities. FlaWARN uses virtual information sharing means, conferences, and training events to review vulnerabilities, provide information, share innovative technologies, and conduct emergency response exercises. Since the FDEP and FDOH are key stakeholders in FlaWARN, they receive important feedback to analyze and, if necessary, bring these issues to the attention of Federal agencies. The FlaWARN system has also proven effective in a host of real-world emergencies across Florida and the Gulf region in 2005, as members provided assistance to an affected region in Texas from Hurricane Rita.

FlaWARN is indeed a coalition of the willing—effectively linking entities with common concerns—allowing a flexible, scalable and responsive approach toward natural disasters and terrorism. The chairman of FlaWARN suggested, "the key would be regional coalitions and some sort of federal-level bridge to work issues, share information, and carry concerns forward."[48] He continued by emphasizing that while national information databases, like the EPA's ISAC, are great resources, they are not being utilized well by the water industry. Instead regional approaches provide the needed face-to-face opportunities for sharing ideas and providing training that is so important in any industry.

FlaWARN is one of many regional coalitions forming across parts of the country to address common issues such as security and disaster response. One other such coalition is the Infrastructure Security Partnership (TISP), a volunteer infrastructure task force linking over 50 stakeholder organizations across the country with a focus on disaster resilience. This Pacific Northwest-based partnership's focus is on collaboration at the local, state and regional levels in sharing information, disaster relief planning and mutual support in case of a disaster. A recent article explains TISP's goal: "to build upon the work of public-private partnerships, interdependencies exercises and lessons learned from past disasters to develop a regional approach that can lead to disaster resilience on a national scale." [49]

While coalitions like FlaWARN and TISP have promise, more must be done at the national-level to integrate the efforts of regional coalitions. Hence, this paper recommends that the Department of Homeland Security and lead federal agencies such as the Environmental Protection Agency take steps toward establishing regional coalitions across the country that specifically address regional challenges, synchronize planning and response efforts, and provide recommendations to the federal government on policy development. This solution builds upon the momentum already underway across the water infrastructure to address terrorism and natural disasters.

Conclusion

Threats to the nation's water infrastructure are as real as any other form of terrorism. Research shows that gaps still remain in effectively understanding the water infrastructure's vulnerabilities and integrating appropriate security measures. The Bush Administration, Congress, the Department of Homeland Security, and the Environmental Protection Agency play key roles in addressing remaining issues. The Administration and Congress must hold the Department of Homeland Security more accountable for leading and integrating the entire water infrastructure security effort. This department is in the best position to fully understand vulnerabilities, develop strategies, focus resources, and integrate planning and response efforts. The Environmental Protection Agency, using the expertise of industry and academia, must develop standards in water monitoring and spearhead rapid monitoring technologies. With the assistance of Congress, the EPA must obtain greater authority in then enforcing these security standards. Finally, the federal government must harness the regional initiatives underway across the water infrastructure. In many cases, regions have a better grasp of their security concerns and best protect their municipalities from terrorism. The DHS and EPA should establish collaborative approaches at the federal level that harnesses regional initiatives, shares information, and shapes more effective security strategies.

While much has been done since 9/11 to protect the nation's water infrastructure, we have only just begun to address the remaining issues with water security. The water infrastructure is complex and expansive and requires full cooperation at all levels to deter terrorist attacks. EPA's Acting Secretary Grumbles was right on the mark when he testified to Congress: "We have good news to report on our progress to date. However, much work remains to be done…"[50] Significant work lies ahead for the U.S. Government, especially the DHS, in orchestrating effective strategies that rapidly analyze evolving threats, that exploits initiatives made by state, local and private organizations, and that effectively integrates security operations across the nation.

Endnotes

[1] George W. Bush, *The National Strategy for Homeland Security*, (Washington, D.C.: The White House, July 2002), 67.

[2] George W. Bush, *The National Security Strategy of the United States of America*, (Washington, D.C.: The White House, September 2002), cover letter.

[3] George W. Bush, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, (Washington, D.C.: The White House, February 2003), 39.

[4] Donald C. Hickman, "A Chemical and Biological Warfare Threat: USAF Water Systems at Risk," *The Counterproliferation Papers, Future Warfare Series No. 3* , September 1999; available from http://www.au.af.mil/au/awc/awcgate/awc-cps.htm; Internet, accessed 18 December 2005.

[5] Yacov Y. Haimes, Nicholas Matalas, James Lambert, Bronwyn Jackson, and James Fellows, "Reducing Vulnerability of Water Supply Systems to Attack", *Journal of Infrastructure Systems*, (December 1998), 164.

[6] H. Court Young, *Practical Guide to Water Supply and Terrorism* , (Denver: Burg Young Publishing, LLC, July 2004), 26.

[7] Benjamin H. Grumbles, Acting Assistant Administrator for Water, U.S. EPA, Statement Before the Subcommittee on Environment and Hazardous Materials Energy and Commerce Committee, U.S. House of Representatives, 30 September 2004, available from http://www.epa.gov/water/speeches/040930bg.pdf; Internet, accessed 18 December 2005.

[8] Hickman, 1.

[9] "How Safe is Our Water? The Threat of Terrorism" (MSNBS Staff and Wire Reports), available from http://www.ionizers.org/water-terrorism.html; Internet, accessed 8 January, 2006.

[10] David Isenberg, "Terrorism—Securing U.S. Water Supplies," (Center for Defense Information, 19 July, 2002), available from http://www.cdi.org/terrorism/water-pr.cfm; Internet, accessed 18 December 2005.

[11] Jeff Stone, "Minimizing Security Risks for Public Water Systems," (University of Arkansas, May 2004), available from http://www.uaex.edu/biosecurity/cross_referenced/public_water.asp; Internet, accessed 18 December 2005.

[12] Ibid.

[13] W. Dickenson Burrows and Sara E. Renner, "Biological Warfare Agents and Threats to Potable Water," *Environmental Health Perspectives*, Volume 107, no. 12 (Dec 1999), 982.

[14] Ibid.

[15] Isenberg.

[16] Kathy Jesperson, "Are Water Systems a Terrorist Target?" *On Tap* (Winter 2002), 16, available from http://www.natat.org/ncsc/Pubs/Newsletter/Feb2002/Quaterly-Winter2002.pdf; Internet, accessed 8 January, 2006.

[17] Mary Tiemann, "Safeguarding the Nation's Drinking Water: EPA and Congressional Actions," Library of Congress, Congressional Research Service, Apr 13, 2005, CRS-1, available from http://www.ncseonline.org/NLE/CRSreports/05oct/RL31294.pdf; Internet, accessed 18 December 2005.

[18] Ibid.

[19] Mary Teimann, “Safe Drinking Water Act: Implementation and Issues,” Library of Congress, Congressional Research Service, July 22, 2005, p. CRS-2, available from http://www.ncseonline.org/nle/crsreports/05Nov/IB10118.pdf; Internet, accessed 18 December 2005.

[20] Claudia Copeland and Betsy Cody, “Terrorism and Security Issues Facing the Water Infrastructure Sector,” Library of Congress, Congressional Research Service, Apr 25, 2005, CRS-1. available from http://www.fas.org/irp/crs/RS21026.pdf; Internet, accessed 18 December 2005; this information is also common knowledge within civil and environmental engineering disciplines and can be found in a host of other technical reports and resources; this information was constantly reinforced over the course of the author’s professional career.

[21] Copeland, CRS-2.

[22] Ibid.

[23] M.D. Ginsberg, V.F. Hock, A.G. Pappas, “Secure Water Supply,” available from http://216.239.51.104/search?q=cache:PhfkNTV2kdMJ:asc2004.com/Manuscripts/sessionF/FP-03.pdf+M.D.+Ginsberg,+V.F.+Hock,+A.G.+Pappas+%22Secure+Water+Supply%22&hl=en; Internet, accessed 18 December 2005.

[24] Burrows, W. Dickenson, “Biological Warfare Agents as Threats to Drinking Water,” (Aberdeen: U.S. Army Center for Health Promotion and Preventive Medicine, 1998) available from http://www.usminstitute.org/content/DBurrows1pager.pdf; Internet, accessed 18 December 2005.

[25] H. Court Young, *Understanding Water and Terrorism* , (Denver: BurgYoung Publishing, LLC, May 2005), 25.

[26] Ginsberg.

[27] Ibid.

[28] David Isenberg, “Terrorism—Securing U.S. Water Supplies,” (Center for Defense Information, 19 July, 2002), available from http://www.cdi.org/terrorism/water-pr.cfm; Internet, accessed 18 December 2005.

[29] William Clinton, White *Paper: The Clinton Administration’s Policy on Critical Infrastructure Protection : Presidential Decision Directive 63,* May 22, 1998, available from http://www.fas.org/irp/offdocs/paper598.htm; Internet, accessed 8 January, 2006.

[30] Bush, *The National Strategy for Homeland Security*, viii.

[31] Bush, 33.

[32] Bush, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, vii.*

[33] Bush, *ix.*

[34] *The National Response Plan,* (U.S. Department of Homeland Security, December 2004), 22, available from http://www.dhs.gov/interweb/assetlibrary/NRPbaseplan.pdf; Internet, accessed 18 December 2005.

[35] *Water Utility Planning Guide, Interim Final*, (U.S. Environmental Protection Agency, December 2003), available from http://www.waterisac.org/epa/Guidance/guide_response_module1.pdf; Internet accessed 18 December 2005, p. 39.

[36] Ibid.

[37] Jeffrey J. Danneels, "Terrorism: Are America's Water Resources and Environment at Risk?" Testimony to Subcommittee on Water Resources and the Environment, Committee on Transportation and Infrastructure, U.S. House of Representatives, 10 October, 2001, 3., available from http://www.house.gov/transportation/water/10-10-01/10-10-01memo.html; Internet, accessed 18 December 2005.

[38] *The National Response Plan*, 80.

[39] Public Law 107-188, *The Public Health Security and Bioterrorism Preparedness Response Act of 2002*, Public Law 107-188, 116 Stat. 294 (2002)

[40] Mary Tiemann, "Safeguarding the Nation's Drinking Water: EPA and Congressional Actions," Library of Congress, Congressional Research Service, Apr 13, 2005, CRS-12, available from http://www.ncseonline.org/NLE/CRSreports/05oct/RL31294.pdf; Internet, accessed 18 December 2005.

[41] EPA Needs to Assess the Quality of Vulnerability Assessments Related to the Security of the Nation's Water Supply," (Office of the Environmental Protection Agency Inspector General, 24 Sep 2003), 4, available from http://www.epa.gov/oig/reports/2003/Report2003M000013.pdf; Internet, accessed 18 December 2005.

[42] Grumbles.

[43] GAO Report, "Experts' Views on How Future Federal Funding Can Best Be Spent to Improve Security", GAO Report to the Committee on Environment and Public Works, U.S. Senate, Oct 2003. 31, available from http://www.gao.gov/new.items/d0429.pdf; Internet, accessed 18 December 2005.

[44] EPA Inspector General Report, "EPA Needs a Better Strategy to Measure Changes in the Security of the Nation's Water Infrastructure" 11 Sep 2003, cover letter, available from http://www.epa.gov/oig/reports/2003/HomelandSecurityReport2003M00016.pdf; Internet, accessed 18 December 2005.

[45] Varu Chilkamarri, "A New Instrument in National Security: The Legislative Attempt to Combat Terrorism via the Safe Drinking Water Act," *Georgetown Law Journal,* April 2003; 91, 4, 947-948.

[46] Bart Bibler, "Protecting Florida's Drinking Water Systems," (Tallahassee: Florida Department of Health), 1, available from http://www.myfloridaeh.org/water/pdfs/WaterTerrorismBrochure.pdf; Internet, accessed 18 December 2005

[47] FlaWARN Website, available from http://www.flawarn.org/; Internet, accessed 18 December 2005.

[48] Phonecon with Mr. Scott Kelly, JEA and Chairman of FlaWARN, Jacksonville, Florida, 12 December 2005.

[49] Paula L. Scalingi, "Disaster Resilience," *Military Engineer Magazine,* 98, No. 639*,* (January-February 2006) Vol. 98, No. 639, 44.

[50] Grumbles.