



OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Evaluation Report

EPA Needs to Assess the Quality of Vulnerability Assessments Related to the Security of the Nation's Water Supply

Report No. 2003-M-00013

September 24, 2003

Report Contributors: Erin Barnes-Weaver
Eric Hanger
Fred Light
Ricardo Martinez
Erin Mastrangelo

Abbreviations

AWWARF	American Water Works Association Research Foundation
CDC	Centers for Disease Control and Prevention
EPA	Environmental Protection Agency
RAM-W	Risk Assessment Methodology for Water



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

OFFICE OF
INSPECTOR GENERAL

September 24, 2003

MEMORANDUM

SUBJECT: EPA Needs to Assess the Quality of Vulnerability Assessments
Related to the Security of the Nation's Water Supply
Report No. 2003-M-00013

FROM: Jeffrey K. Harris /s/
Director for Program Evaluation, Cross-Media Issues

TO: Tracy Mehan
Assistant Administrator for Office of Water

In connection with our ongoing evaluation of the Environmental Protection Agency's (EPA's) activities to enhance the security of the Nation's water supply, we noted an issue that requires your immediate attention. Specifically, we believe EPA should promptly analyze the vulnerability assessments submitted by large utilities pursuant to the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 ("Bioterrorism Act") to determine whether the assessments adequately and comprehensively address terrorist threats.

We propose this action because, during our preliminary research,¹ we obtained information that suggests that problems may exist in:

- Identifying and prioritizing specific threats – particularly terrorist scenarios; and
- Assessing the full breadth of a water system's infrastructure – particularly its distribution system.

It is important that EPA promptly implement improvements to the vulnerability assessment process. According to an EPA official, although approximately 400 large utilities already submitted their vulnerability assessments, thousands of additional assessments are due from medium-sized water systems before the end of 2003 and from small-sized utilities by mid-2004.

¹The EPA Office of Inspector General is conducting preliminary research on an evaluation of water system security activities in support of the Agency's Strategic Plan for Homeland Security.

Therefore, we determined that our observations were significant enough to report to you at this time because of the time-critical nature of the issues discussed below. The Bioterrorism Act authorized \$160 million for fiscal year 2002 – and such sums as may be necessary for fiscal years 2003 through 2005 – to fund water security activities, including the vulnerability assessments, and Congress may base future funding decisions on those assessments.

Our observations and suggestions are based on information obtained from our interviews with water security experts, water utility officials, and EPA headquarters and regional representatives; attendance at water vulnerability assessment training; and a review of vulnerability assessment tools, methodologies, and related documents. We are performing our evaluation in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States.

Vulnerability Assessments Provide Foundation for Emergency Response

The nation's water supply is one of our most vital natural resources. Potential threats to this resource include contamination with biological, chemical, or radiological agents, or destruction of physical infrastructure. Presidential Decision Directive 63, issued in May 1998, designated EPA as the lead agency for assuring the protection of the nation's water infrastructure. The terrorist attacks on September 11, 2001 ("9/11") resulted in passage of the Bioterrorism Act and its requirement that water utilities submit vulnerability assessments to EPA. EPA's strategy for improving water security relies on water utilities to conduct vulnerability assessments, develop or modify emergency response plans, and institute security enhancements. EPA facilitates these actions by developing assessment tools and training, compiling a single threat summary, and providing financial assistance directly to large drinking water systems to conduct vulnerability assessments and to States for medium- and small-sized utilities.²

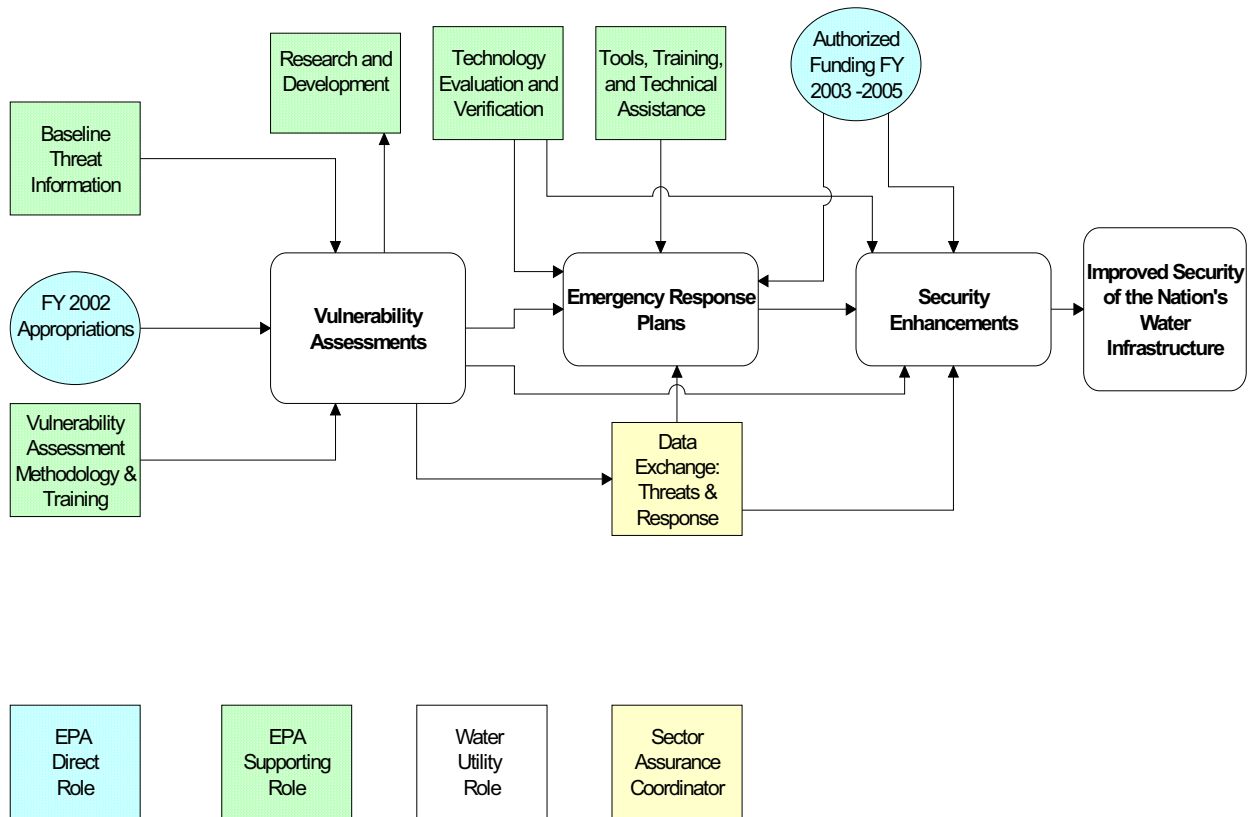
Figure 1 illustrates that vulnerability assessments serve as the foundation for emergency response plans and future security enhancements implemented by water utilities. EPA's November 2002 *Vulnerability Assessment Factsheet* notes that vulnerability assessments help water systems evaluate susceptibility to potential threats and design response plans and corrective actions to lessen the risk of serious consequences. EPA's *Factsheet* further states that an effective vulnerability assessment serves as a guide to the water utility by providing a prioritized plan for security upgrades, modifications of operational procedures, and/or policy changes to reduce risks to a utility's critical assets. A water security expert at Sandia National Laboratory³ said that utilities use vulnerability assessments to help determine how well water systems detect security problems and stop or delay undesired events, as well as measure response capabilities. In

²Following the terrorist attacks of 9/11, EPA received supplemental fiscal 2002 funding of \$89 million to improve the safety and security of the Nation's water supply. EPA used \$53 million of that funding to provide grants to the largest water utilities (those that serve 100,000 or more people) to assist them in conducting vulnerability assessments. EPA also provided \$21 million in grants to assist States in improving drinking water security for medium utilities (serving between 50,000 and 99,999 people) and small utilities (serving between 3,300 and 49,999 people).

³A Government-owned facility operated by a contractor for the U.S. Department of Energy's National Nuclear Security Administration.

addition to water utilities, vulnerability assessments are routinely used to develop response plans to address threats to chemical facilities, computer systems, nuclear weapons facilities, the electrical power industry, and wastewater treatment plants. Figure 1 also illustrates EPA's efforts in the water security area and shows the Agency's primary role in providing vulnerability and threat assessment assistance.

Figure 1: Water Security Concept Model



The Bioterrorism Act required that utilities serving a population greater than 3,300 persons conduct and submit their vulnerability assessments to EPA according to deadlines based on a utility's size.⁴ Water utilities may conduct their assessments using one of several different methodologies. EPA provided funding to Sandia National Laboratory and the American Water Works Association Research Foundation (AWWARF) to develop training on the Risk Assessment Methodology for Water (RAM-W). RAM-W is one tool utilities can use to

⁴Water utilities serving 100,000 or more users had to submit their assessments by March 31, 2003; mid-sized utilities serving between 50,000 and 99,999 users must submit their assessments by December 31, 2003; and small utilities serving between 3,300 and 49,999 users must submit their assessments by June 30, 2004.

systematically assess vulnerabilities to terrorist and other intentional attacks. The RAM-W program stems from a vulnerability assessment methodology initially developed by Sandia to support the national nuclear security mission and from Sandia's involvement in the development of a risk assessment approach for dams. Sandia provided RAM-W training workshops under an interagency agreement with EPA. While EPA focused its efforts on the development of RAM-W, water utilities have other methodologies available to assist them in conducting their vulnerability assessments. EPA provided assistance to the Association of Metropolitan Sewerage Agencies, the Association of State Drinking Water Administrators, and the National Rural Water Association to develop similar tools to help medium and small utilities assess threats to their water systems.

Regardless of the methodology used, the Bioterrorism Act identified six elements that water utilities must address in their assessments of vulnerabilities to a terrorist attack or other acts intended to substantially disrupt the ability to provide a safe and reliable supply of drinking water:

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

EPA issued guidance to utilities interpreting the Bioterrorism Act's six elements in the Agency's November 2002 *Vulnerability Assessment Factsheet*. While EPA did not specify a particular format or methodology for the vulnerability assessments, EPA emphasized that the following guidance applies to the vulnerability assessments conducted by all water utilities regardless of the size of the population served:

- (1) Characterization of the water system, including its mission and objectives.
- (2) Identification and prioritization of adverse consequences to avoid.
- (3) Determination of critical assets that might be subject to malevolent acts that could result in undesired consequences.
- (4) Assessment of the likelihood (qualitative probability) of such malevolent acts from adversaries.
- (5) Evaluation of existing countermeasures.
- (6) Analysis of current risk and development of a prioritized plan for risk reduction.

Vulnerability Assessments May Not Necessarily Address Terrorist Threats

The Bioterrorism Act requires community water systems to prepare for and assess vulnerabilities to terrorist and other intentional acts. However, based on our interviews, we believe that vulnerability assessments submitted may emphasize traditional, less consequential, and less costly threats, such as vandalism or disgruntled employees. Therefore, vulnerability assessments

may not necessarily address terrorist scenarios or the events of 9/11 that motivated passage of the Bioterrorism Act.

The assessment of vulnerabilities is a threat-driven exercise where the design of response actions are dependent upon the credibility of the defined threat. Neither the Bioterrorism Act nor EPA identified a minimum threat level against which water utilities should assess their vulnerabilities. Water security experts view understanding the threat as the driver to vulnerability assessment methodologies. However, EPA provided limited threat information that resulted in utility managers having to determine threats and response actions themselves. The RAM-W methodology instructed managers to define their system-specific threat by considering their own operational, legal, and financial limitations against the threat information provided by local intelligence sources.

Water security experts we interviewed stated that EPA did not provide adequate threat information. Officials at Sandia National Laboratory stated that EPA's threat guidance missed the mark because EPA did not set a minimum threat level against which utilities needed to assess their vulnerabilities. One AWWARF official found EPA's threat guidance too general and believed it lacked information utilities could act upon. For example, the document left responsibility to the utilities in defining subjective terms such as "reasonable protective measures." The AWWARF official further stated that EPA made no effort to provide credible threat information to utilities who needed it. The official said that although the Centers for Disease Control and Prevention (CDC) worked on compiling a list of potential contaminants, neither EPA nor CDC distributed this information to utilities. Although EPA incorporated the CDC information into the Agency's State of Knowledge report on contaminant threats, EPA officials considered that report to be too sensitive to share with decision-makers, including utility managers and congressional staff. Consequently, the AWWARF official noted that the Bioterrorism Act tasks utilities with conducting vulnerability assessments without proper credible threat information from EPA.

In the absence of credible threat information from EPA, water utility staff decided for themselves what threats to include in their vulnerability assessments. For example, one water security expert, contracted to conduct vulnerability assessments for many large water systems, said that, despite the RAM-W training provided after 9/11, water utilities focus on vandals, criminals, and disgruntled employees in their vulnerability assessments. The contractor further stated that EPA has not provided utilities the intelligence data or threat information required to justify the security upgrades necessary to defend against terrorism.

While the terrorist attacks of 9/11 and the subsequent passage of the Bioterrorism Act served as the catalyst for the vulnerability assessments, limited threat information provided by EPA resulted in utilities subjectively designing their assessments around pre-9/11 threats. All of the utilities and contractors we interviewed used the RAM-W methodology to complete their vulnerability assessments. After filtering threat information through the RAM-W methodology, most of the water security experts we interviewed who were familiar with vulnerability assessments concluded that the only threats utilities could realistically address were those they encountered before 9/11. One utility representative we interviewed said that the contractor they

hired to conduct their vulnerability assessment discouraged them from addressing higher threat levels like terrorism.

Assessment Guidance Does Not Emphasize Unique Water System Vulnerabilities

Neither EPA nor the vulnerability assessment methodologies provided threat guidance that identified the most vulnerable components unique to water systems. The lack of clear guidance on what components to focus on resulted in utility managers deciding for themselves whether to emphasize the vulnerabilities of components, such as distribution systems. This results in inconsistent assessments and response actions, and may prevent EPA from ensuring future improvements to water security.

Many experts view water distribution systems as the most susceptible to terrorist attack. Such experts included the President of the Association of Metropolitan Water Agencies, who concluded that water distribution systems remain the most vulnerable to terrorist threats and could spread highly concentrated amounts of poison to a few thousand homes or businesses. The Chair of the National Academy of Sciences' Water Science and Technology Board also found water distribution systems difficult to secure and recognized that, while such systems may affect a smaller population, mass exposure is not needed if the terrorists' goal is fear and anxiety. As a result, public reports of illnesses may be the earliest indicator of deliberate contamination to distribution systems, according to one vulnerability assessment contractor.

A State water security coordinator said that neither EPA nor the different methodologies adequately emphasized distribution system threats as the most susceptible components of water systems to include in vulnerability assessments. While the RAM-W methodology acknowledges the susceptibility of threats to distribution systems, the methodology only mentions distribution systems as one of the many critical assets utility managers should seek to protect. Sandia's RAM-W program stems from a vulnerability assessment methodology initially developed to support the national nuclear security mission. The methodology has since been modified to evaluate the vulnerability to terrorist attack of government buildings, Air Force bases, nuclear power plants, nuclear processing facilities, prisons, and Federal dams. The State water security coordinator further said that RAM-W, as an artifact of nuclear- and dam-based methodologies, may be inappropriate for water utilities given their multiple facility size, unique and often elaborate distribution systems, and interconnections with other sectors.

Suggestions

EPA has plans to sample the vulnerability assessments to ensure compliance with Bioterrorism Act requirements. Based on our observations, we offer the following suggestions:

- (1) EPA should consider including in its review a qualitative analysis of vulnerability assessments submitted by large utilities to determine whether they adequately address the threats envisioned by the Bioterrorism Act. Specifically, EPA's analysis should address whether the large utilities:
 - a. identified and prioritized specific threats – particularly terrorist scenarios; and
 - b. assessed the full breadth of a water system's infrastructure – particularly its distribution system.
- (2) If EPA's analysis confirms our observations, EPA should focus on amending its guidance to address the shortcomings identified in this memorandum.

Agency Comments and Office of Inspector General Evaluation

In response to the concerns raised in our draft report, EPA analyzed a sample of the large water utility vulnerability assessments to determine if they specifically identified and addressed terrorist scenarios and distribution systems. EPA stated that any lessons learned from this analysis would be incorporated into guidance and training for medium and small water systems. Given that vulnerability assessments serve as the foundation for emergency response plans and future security enhancements, the OIG suggests that EPA monitor all water system submissions to ensure that vulnerability assessments identify and prioritize specific threats – particularly terrorist scenarios; and assess the full breadth of a water system's infrastructure – particularly its distribution systems.

The full Agency response is provided in Appendix A.

- - -

If you or your staff have any questions regarding this report, please call me at (202) 566-0831.

Agency Response



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

JUN 16 2003

OFFICE OF
WATER

MEMORANDUM

SUBJECT: Response to OIG Concerns Regarding the Quality of Vulnerability Assessments
Related to the Security of the Nation's Water Supply

DRAFT: Report No. 2003-M-000013

FROM: G. Tracy Mehan, III /s/
Assistant Administrator

TO: Jeffrey K. Harris
Director for Program Evaluation, Cross-Media Issues
Office of Inspector General

I am responding to the issues and concerns presented in your May 16, 2003, memorandum/report to me on the evaluation of the Environmental Protection Agency's (EPA) activities to enhance the security of the Nation's water supply. You specifically emphasized that EPA should promptly analyze the vulnerability assessments submitted by large utilities, as required by the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 ("Bioterrorism Act"), to determine whether the assessments adequately and comprehensively address terrorist threats. In this analysis, you suggested that EPA consider a qualitative review of whether the large utilities:

- a. identified and prioritized specific threats – particularly terrorist scenarios; and
- b. assessed the full breadth of a water system's infrastructure – particularly its distribution system.

I understand that you made these suggestions because your preliminary research indicates there could be omissions in these areas. If that is the case, you propose that the Agency issue amended guidance to drinking water systems on conducting vulnerability assessments.

I believe that you and your staff would benefit greatly from a comprehensive briefing of the Water Protection Task Force's efforts over the past 20+ months. Your report focuses on the

reactions of numerous stakeholders to EPA's activities, so I encourage you and your staff to learn of them first hand from the Task Force's staff.

Development of Baseline Threat and Vulnerability Assessment Guidance

Since your memorandum/report cites interviews and discussions with many representatives in the drinking water community, I want to reiterate EPA's approach in developing the guidance to water utilities on assessing vulnerabilities to terrorist attacks and other intentional acts. First, the water industry, the federal public health, military, agricultural and food sectors, as well as the intelligence and law enforcement community were closely involved in identifying and defining risks to public health in relation to such attacks/acts. This was a critical step in both assisting utilities in developing their baseline threats for vulnerability assessments and in determining vulnerabilities in a distribution system relative to other infrastructure components of a water system. We also had a comprehensive process for developing tools and guidance on available baseline threat information that culminated in a meeting of national stakeholders in the Summer of 2002. This meeting was conducted to solicit feedback on issues relevant to conducting vulnerability assessments as well to reviewing and commenting on baseline threat concerns. In attendance were water industry officials from the Association of State Drinking Water Administrators (ASDWA), which represents the State primacy agencies, the American Metropolitan Water Agency (AMWA), which represents large water systems, and the American Water Works Association (AWWA), which represents the drinking water utilities, and managers/staff of several large municipalities including the Metropolitan Water District of Southern California and the City of Newport News, VA. The FBI sent experts from its National Infrastructure Protection Center to speak and act on behalf of the federal law enforcement sector and other sectors were represented by participants from the FDA, CDC, USDA and the US Army.

The primary purpose of this stakeholder meeting was to discuss a draft version of the *Baseline Threat Information for Vulnerability Assessments of Community Water Systems* (Baseline Threat Document) that was distributed to participants beforehand. This document was drafted to provide utility managers and their staffs with information necessary for the appropriate identification and evaluation of vulnerabilities, threats, and kinds of attack that could place the operation of the water utility (including the distribution system components), staff, and customers in harms way. One chapter of this document, *Determining The Level of Threat*, focused heavily on consideration of the terrorist threat as well as the national resources that are available to utilities to obtain threat information, e.g., the water information sharing and analysis center (WaterISAC). (Although in its infancy, the WaterISAC will provide utilities secure, timely, useable information to support efforts to protect the Nation's water infrastructure.) According to my staff, discussion of this chapter was active and intense especially around the FBI's assertion that intelligence on terrorist attacks is much more up-to-date and utility-specific at the field office level. As a result, the prevailing position of the stakeholders was that the design basis threat selection should be left to individual utilities to account for the uniqueness of

each water system while incorporating the threat information gained from local FBI field offices and other security experts. Thus, this chapter in the final guidance presents a general description of the full range of threats, the historical threat perspective of the intelligence community (including input from the AWWArf and Sandia National Laboratories), and the specific recommendation that utilities seek participation and insight from local levels of law enforcement as they conduct their vulnerability assessments.

More extensive information - - in the form of appendices to the Baseline Threat Document - - on contamination threats and vulnerabilities was made available to utility managers. Most large utilities took advantage of this information as they conducted their vulnerability assessments as are medium and small systems that are currently conducting their assessments. While these materials cannot leave the secured area in which they are stored and filed, you and your staff can read and review this document and appendices by contacting the Water Protection Task Force.

Scope of Vulnerability Assessments

EPA agrees with the experts you interviewed that contamination of the distribution system could result in serious public health episodes. In our negotiations and discussions with the stakeholder organizations to which EPA provided financial support for the development of methodologies and tools for conducting vulnerability assessments, Agency officials highlighted this important area to reinforce and augment the RAM-W methodology with respect to distribution systems. An EPA official attended the train-the-trainer workshop and pointed out to the trainees that they would need to go beyond the focus of this methodology on distribution systems in order to consider and assess the vulnerabilities of the entire distribution system. At the same time, our intent for all the workshops we supported in 2002 was to concentrate on particular, high priority, areas of vulnerability in drinking water infrastructure and also give sufficient attention to all other areas as well. The Bioterrorism Act requires system evaluation as a whole and any emphasis on the distribution system without proper consideration or endorsement of the entire system could diminish the review of other vulnerable system components.

Also, I think it is important to recognize that security of the water sector, like all other sectors comprising homeland security, is a highly dynamic and evolving arena. Conducting vulnerability assessments should not be considered a one time endeavor but instead an iterative activity that water systems will have to review and update on a regular basis. EPA's approach to and support of current and future training on methodologies and tools for conducting vulnerability assessments of water systems will reflect "lessons learned" from 2002 and will incorporate state-of-the-art approaches developed in the interim.

Ongoing Assistance to Water Utilities

EPA's ongoing efforts in water infrastructure protection emphasize and support both

research on contaminant monitoring approaches and technical assistance for water utilities and emergency response providers to act in response to contamination of water supplies. Workshops that will assist systems, serving between 50,000 and 100,000 people, in conducting their vulnerability assessments will be underway next month. Information and tools to address and strengthen action against identified vulnerabilities to attack and/or to disrupt water service entirely are continually being developed and implemented. For instance, the Agency is currently supporting the dissemination of a hydraulic model capable of predicting fate and transport of contaminants in distribution systems. This model is coupled with GIS tools to allow a system to identify locations that could be seriously affected by a “contamination event” and to develop appropriate proactive as well as response plans. A research strategy, developed jointly by the Office of Water, the Office of Research and Development and major stakeholders in the water community, will be published in the near future. This strategy contains an impressive mix of projects that cover a wide range of water security-related basic research as well as the development of technologies to detect, minimize, and protect against the introduction of harmful contaminants into water supplies.

Review of Vulnerability Assessments

I have already carried out one of the suggestions in your report. Staff (with top secret clearance) of the Water Protection Task Force has completed a qualitative review of a subset of the vulnerability assessments submitted by large drinking water systems. OW can brief you on the results of this review once you have been designated by the Administrator in accordance with the requirements of the Bioterrorism Act. As stated previously, my staff is ready to give you a full and detailed account of water security activities.

I appreciate the opportunity to respond to your draft report. Should you have any questions or need additional information, please contact Judy Hecht, the Office of Water’s liaison to the IG’s office, on 564-0475.

Distribution

Acting Administrator
Associate Administrator for Congressional and Intergovernmental Relations
Acting Associate Administrator, Office of Public Affairs
Assistant Administrator, Office of Water
Audit Followup Coordinator, Office of Water
Director, Office of Ground Water and Drinking Water
Chair, Water Protection Task Force
General Counsel
Director, Office of Homeland Security