

SECURITY

Insight Into the Regulation

Our world and the way we operate our water systems has changed since September 11, 2001. Prior to that date, however, efforts to protect critical infrastructures in our country were already underway. Presidential Decision Directive 63 (PDD-63), issued in 1998, identified the water supply as one of eight critical infrastructures. There is now national effort in progress to institute preventative and quick response measures for these critical infrastructures to assure the continued health and well-being of the United States of America and its citizens.

In June 2002, Congress passed the Public Health Security and Bioterrorism Preparedness Act of 2002 (Public Law 107-188). This law requires water systems serving greater than 3,300 to prepare and submit to USEPA an assessment of system vulnerability to terrorist attack.

There are no specific requirements in terms of the level of detail required for the vulnerability assessments provided that the required six elements are addressed. It has been advised that utilities prepare their vulnerability assessments based on the guidance of Counsel as well as EPA input.

Regardless of the methodology employed, systems should take care to safeguard all sensitive information.

Go to www.epa.gov/safewater/security for more information on security issues.

Federal Regulatory Requirements

1. VULNERABILITY ASSESSMENT: As stated in the law, vulnerability assessments (VAs) must 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 system. A copy of the completed VA must be submitted to the USEPA by:

- a. March 31, 2003 if serving 100,000 or more people
- b. December 31, 2003 if serving 50,000 or more but less than 100,000
- c. June 30, 2004 if serving more than 3,300 but less than 50,000

Methodology: Large Systems (Serving >100,000)

The American Water Works Association Research Foundation and USEPA sponsored the development of a Risk Assessment Methodology for Water (RAM-WSM) through Sandia National Laboratories. The methodology is a step-wise protocol for conducting a high-level review of the entire water system. The RAM-WSM methodology involves the identification of physical and cyber threats and a systematic review of all critical facilities and critical assets based on the anticipated threat in a manner that results in a prioritization of vulnerable assets. The methodology is performed by a core team composed of water system personnel, water system experts, security experts, and other subject matter experts as appropriate. The intent is that the methodology will be revisited as improvements are made and that over time the system will continually re-evaluate and effectively reduce its risk to terrorist attack.

Methodology: Medium Systems (Serving 50,000 - 100,000)

Working with the USEPA, the Association of Metropolitan Sewerage Agencies (AMSA) developed Vulnerability Self-Assessment Tool (VSATTM) software for small and medium water systems and wastewater systems. This software is available free to all public utilities. Sandia National Laboratories and the USEPA have also developed a scaled-down version of the RAM-WSM methodology for small and medium systems, RAM-WTM Lite. Although the USEPA does not specify a required methodology, VAs must contain the following six elements:

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; and
6. Analysis of current risk and development of a prioritized plan for risk reduction.

(continued)



If you have any questions on the information provided in this handout or additional questions concerning USEPA drinking water regulations, contact Wayne Gerszewski, PE at 701-746-8087 (Grand Forks), Russ Sorenson, PE at 701-221-0530 (Bismarck), Grant Meyer, PE at 763-463-5036 (Minneapolis), Nate Weisenburger, PE at 406-268-0626 (Great Falls), or Brian Bergantine, PE at 218-299-5610 (Moorhead).

SECURITY

Federal Regulatory Requirements

Methodology: Small Systems (Serving 3,300 - 49,999)

The Association of State Drinking Water Administrators and the National Rural Water Association, in collaboration with the USEPA, have developed a “Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems.” This document, designed for systems serving populations of 10,000 or less, provides a starting point for small systems to determine possible vulnerable components of their systems, even though systems of this size are not required by law to conduct a vulnerability assessment.

2. EMERGENCY RESPONSE PLAN: Public Law 107-188 also requires systems to develop an Emergency Response Plan or to revise an existing plan, incorporating the findings of the vulnerability assessment. Systems must certify completion of the Emergency Response Plan requirement to the USEPA within 6 months of completion of the vulnerability assessment, but are not required to submit a copy to the USEPA. Utilities must coordinate to the extent possible with Local Emergency Planning Committees in preparing plans.

3. SECURITY ENHANCEMENTS: The findings of the vulnerability assessment are intended to assist the utility in prioritizing system security upgrades.

4. FREEDOM OF INFORMATION ACT (FOIA): Congress has exempted vulnerability assessments from the FOIA at the federal level. There are concerns, however, as to local Sunshine laws at the state level. During the Fifty-Eighth Legislative Assembly of North Dakota, HB 1143, which relates to the confidentiality of public health and security system plans, was introduced. HB 1143 was passed by the Legislature, and exempts vulnerability assessments from local Sunshine Laws.

5. SMALL AND MEDIUM SYSTEM STRATEGY: The USEPA had identified a strategy for small and medium systems. The strategy outlines the objectives for addressing drinking water system and wastewater utility security needs as:

- a. Providing tools and guidance to drinking water systems and wastewater utilities.
- b. Providing training and technical assistance, including “train-the-trainer” programs.
- c. Providing financial assistance to undertake vulnerability assessments and emergency response plans as funds are available.
- d. Build and maintain reliable communication processes.
- e. Build and maintain reliable information systems.

f. Improve the knowledge of potential threats, methods to detect attacks, and effectiveness of security enhancements in the water sector.

g. Improve networking among groups involved in security-related matters -- water, emergency response, laboratory, environmental, intelligence, and law enforcement communities.

6. WATER INFORMATION SHARING AND ANALYSIS CENTER (ISAC):

In addressing PDD-63, the USEPA was identified as the lead federal agency for the water sector. The Association of Metropolitan Water Agencies (AMWA) has been appointed by the USEPA to coordinate the efforts to protect the water infrastructure. In coordination with the FBI and the USEPA, the AMWA is developing a water ISAC, which will be a secure means for communicating information such as threats that have been detected, vulnerabilities that have been discovered, viable resolutions to incidents, threats, and vulnerabilities, reports of incidents that have occurred, etc. Membership is voluntary, available to systems within the United States, and requires application approval and an annual membership fee based on population served.

SECURITY: AN EVOLVING PROCESS WITH EVOLVING REQUIREMENTS AND FUNDING PROSPECTS.

Process: In addressing the issue of water system security, it is important to embrace the idea that improving the security of our systems is not a one-time effort to comply with PL107-188, but a continual process. As changes to systems are made, utilities must re-evaluate their vulnerability and adjust security upgrade priorities accordingly to ensure that over time, the effective risk to the system is reduced.

Funding: In response to the attacks of September 11, Congress provided the USEPA with a \$90 million supplemental appropriation to improve the safety and security of the nation’s water supply. The USEPA allocated \$53 million of that appropriation for \$115,000 grants to each water utility serving greater than 100,000 people to meet the requirements of PL107-188. Funding for small and medium water systems to date has come in the form of training, software, and technical assistance.