Catalyst for Improving the Environment

Evaluation Report

Survey Results on Information Used by Water Utilities to Conduct Vulnerability Assessments

Report No. 2004-M-0001

January 20, 2004

Abbreviations

AWWA   American Water Works Association

CDC   Centers for Disease Control and Prevention

DHS   Department of Homeland Security

DWG   Domestic Working Group

EPA   Environmental Protection Agency

FBI   Federal Bureau of Investigation

Water-ISAC   Water Information Sharing and Analysis Center

NRWA   National Rural Water Association

SCADA   Supervisory Control and Data Acquisition

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

January 20, 2004

MEMORANDUM

SUBJECT: Survey Results on Information Used by Water Utilities to Conduct Vulnerability
                       Assessments

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

TO: Benjamin Grumbles
                       Acting Assistant Administrator for Office of Water

Recent terrorist activities and incidents such as the blackout in the midwest and northeast United
States have demonstrated the crucial role of water sector infrastructures in the health and
economic well-being of the Nation. The Environmental Protection Agency (EPA) is the lead
Federal agency for safe drinking water and for protecting the infrastructure that supplies water.
While EPA has made efforts to prepare water utilities for dealing with terrorist activities, the
goal of a secure water supply needs the participation and coordination of water utilities with
Federal, State, and local agencies.

Recognizing that Federal, State, and local levels of government have a vested interest in water
security, we suggested that the Domestic Working Group (DWG)[1], an informal group of Federal,
State, and local auditors, develop a survey focusing on the security needs and tools of their local
water systems. The objective of the survey was to gather feedback on the usefulness of water
security information provided to utilities by EPA and other sources. Specifically, the survey
helped determine the following:

'   Did EPA and other Federal, State, and local agencies provide useful threat and risk
           information to water utilities to conduct vulnerability assessments as required by the
           Public Health Security and Bioterrorism Preparedness and Response Act of 2002
           ("Bioterrorism Act")?

---

[1]Individual DWG members volunteer to work on issues of common interest. Each organization conducts
work individually that forms the foundation for specific organization audits that can be compiled to support a more
generalized assessment or benchmark.

, What are the needs of utilities with regard to financial assistance, training, and procedural changes to improve security?

, What information can be collected and analyzed by EPA that would depict changes in security levels at water utilities?

This report contains details on what we found regarding these questions, and we included the survey itself in Appendix A. We provided this report to the Agency for comment and the Agency did not provide a response.

If you or your staff have any questions, please call me at (202) 566-0831 or Fred Light at (913) 551-7528.

Table of Contents

Sections

Appendices

Figures

Introduction

Members of the DWG surveyed their local water utilities regarding (1) the usefulness of water security information in conducting vulnerability assessments, (2) remaining security needs, and (3) potential measures to track progress in water security. Though the results of the DWG survey cannot be interpreted as representing conditions within the water industry or the Nation due to limitations of the sample, agencies overseeing efforts to enhance the security of the Nation's drinking water infrastructure, such as EPA, may benefit from the observations. For example, the survey shows that, while EPA and groups such as the American Water Works Association (AWWA) provided useful information, the survey respondents most frequently listed consultants hired by water utilities as providing useful information. This suggests a possible disadvantage to smaller utilities which are required to complete vulnerability assessments by June 2004 but, unlike larger utilities, may not be able to afford a consultant.[2]

In addition, each of the utilities surveyed had concerns for water security that included: the information available to assess vulnerabilities; the financing of security improvements; the level of training assistance; EPA's research agenda; and the need for procedural changes. For example, the Water Information Sharing and Analysis Center (Water-ISAC)[3] can provide utilities useful threat information, but water utilities can only access Water-ISAC through a subscription fee. Survey respondents also stated that they needed financial assistance for necessary security enhancements, training exercises to prepare for actual events, and research to detect contaminants in the distribution system.

The survey found that EPA could use the following performance indicators to measure changes in water security levels:

1. Length of time a water utility could provide water during or after a security incident.
2. Detection and response times.
3. Ability to detect contaminants in the water system.
4. Ability to detect attempted intrusions into the remote access system, commonly known as the Supervisory Control and Data Acquisition (SCADA) system.

---

[2]EPA provided $53 million in grants to over 400 large water utilities that primarily used the grant money to hire water security consultants to assist in conducting vulnerability assessments. EPA also provided $21 million in grants to provide drinking water security training to over 8,000 small and medium water utilities.

[3]The Association of Metropolitan Water Agencies developed the Water-ISAC with funding from EPA as an information service to provide the Nation's drinking water systems with a secure Web-based environment for early warning of potential threats and a source of knowledge about water system security. Water-ISAC analysts produce and disseminate physical and cyber security information to the water sector relying on information gathered from Federal intelligence, law enforcement, public health and environment agencies, and utility security incident reports. Utilities access the Water-ISAC on a subscription fee basis.

Background

The Nation's water supply serves as one of our most vital natural resources. Potential threats to this resource include contamination with biological, chemical, or radiological agents, or damage and destruction of the water system. Despite concerns from industry and Congress that the Federal government should not require specific approaches for water security, and that local water utilities should develop solutions themselves, EPA plays an important role in the security of the Nation's water supply. Presidential Decision Directive 63, issued in May 1998, designated EPA as the lead agency for assuring the protection of the Nation's water infrastructure. Homeland Security Presidential Directive / HSPD-7, issued in December 2003, confirms EPA's role as the lead agency for drinking water and water treatment systems. The terrorist attacks on September 11, 2001, resulted in passage of the Bioterrorism Act and its requirement that water utilities conduct vulnerability assessments.[4]

Vulnerability assessments help water systems evaluate susceptibility to potential threats and design response plans and corrective actions to lessen the risk of serious consequences. Vulnerability assessments help determine how well water systems detect security problems and stop or delay undesired events, as well as measure response capabilities.

EPA developed a Strategic Plan for Homeland Security ("Plan"), dated September 2002, which states that EPA will work with the States, tribes, drinking water utilities, and other partners to enhance the security of water utilities. The Plan articulates tactics to execute the Plan which include the provision of tools, training, and technical assistance to help water utilities' conduct vulnerability assessments, implement security improvements, and effectively respond to terrorist events.

Scope and Methodology

To learn about the usefulness of information water utilities received from EPA and other Federal, State, and local agencies, the DWG developed, pre-tested, and administered a *Survey of Water Security* (see Appendix A). We conducted our review in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. Each DWG auditor administered the survey to their local water utility,[5] and the EPA Office of Inspector General compiled the individual surveys and summarized the results in this report. Due to concerns about releasing sensitive water utility information under a Freedom of Information Act request, the DWG participants made an overt choice <u>not</u> to inquire about specific sensitive vulnerability

---

[4]The Bioterrorism Act required that water utilities serving a population greater than 3,300 persons conduct vulnerability assessments according to a utility's size. Water utilities serving 100,000 or more users had to conduct their assessments by March 31, 2003; mid-sized utilities serving between 50,000 and 99,999 users had to conduct their assessments by December 31, 2003; and small utilities serving between 3,300 and 49,999 users must conduct their assessments by June 30, 2004.

[5]Six separate auditors conducted surveys at six different water utilities; one auditor conducted the seven New York surveys; one auditor conducted two of the California surveys; and one water utility volunteered to provide survey information, for a total of 16 surveys.

information. Six of the 22 water utilities decided not to participate in the survey due to concerns regarding the release of information to the public.

Water utilities have a number of information sources available to assist them in conducting vulnerability assessments. We asked utilities to provide an assessment of the usefulness of the information obtained from the following sources:

- Environmental Protection Agency (EPA)
- Federal Bureau of Investigation (FBI)
- Department of Homeland Security (DHS)
- Centers for Disease Control and Prevention (CDC)
- Other Federal Agencies
- State Agencies
- Local Law Enforcement
- Water Information Sharing and Analysis Center (Water-ISAC)
- InfraGard[6]
- National Rural Water Association (NRWA)
- American Water Works Association (AWWA)
- Water Consultant Hired by Utility
- Water Security Expert

The survey requested information from water utilities in the following areas:

- *Usefulness of information obtained from EPA and other Federal, State and local agencies to conduct vulnerability assessments.* The survey asked respondents to rate their satisfaction on a scale of "1" (Not Very Useful) to "5" (Very Useful).

- *Resources and training needed by water utilities.* The survey asked respondents to provide needed information and resources to better improve the security of their water systems from terrorist attack.

- *Data and performance measures that could track changes in water security levels.* The survey asked respondents to provide suggestions for these measures.

Limitations of the Survey

It is important to note that the survey results represent only the opinions of 16 water utilities, including seven from the State of New York, and should not be generalized to represent all water utilities nationally. We analyzed the survey data and did not find that the seven utilities from New York State provided similar responses which would have disproportionately influenced the results. In addition, the performance indicators suggested may not be comprehensive since they

---

[6]InfraGard is an information sharing and analysis effort led by the FBI and an association of businesses, academic institutions, and State and local law enforcement agencies. InfraGard provides private sector infrastructure owners and operators information about cyber intrusions, exploited vulnerabilities, and infrastructure threats.

are based on a sample of utilities that may not have experience with performance measurement and may have been influenced by the examples in the survey. While limited to 16 utilities, we believe the survey results presented in this report could help EPA, other agencies, and water utilities focus their efforts on the security issues identified. Also, State and local DWG auditors may find the survey responses of particular interest given that they administered the survey and may have oversight responsibilities for their local water utilities. It is not our intention to critique the judgments of individual water utilities or sources who provided the information.

Characteristics of the Survey Population

The 16 water utilities surveyed in six States identified in Figure 1 represent various geographical areas, size of populations served, and stages in the vulnerability and emergency response process.

The utilities surveyed ranged in the size of populations served. Four utilities surveyed serve small populations of 3,300 - 99,999 users, while 12 utilities surveyed serve large populations of greater than 100,000 users.

Of the 16 utilities surveyed, 14 have completed the vulnerability assessment process, and 15 used consultants to assist in the preparation of vulnerability assessments. The remaining utility represented the smallest survey respondent and the superintendent of its water plant conducted their vulnerability assessment. Six of the utilities have also completed their emergency response plans. Only one of the utilities has completed implementing its security enhancements.

Figure 1: Number and Locations of Utilities Surveyed
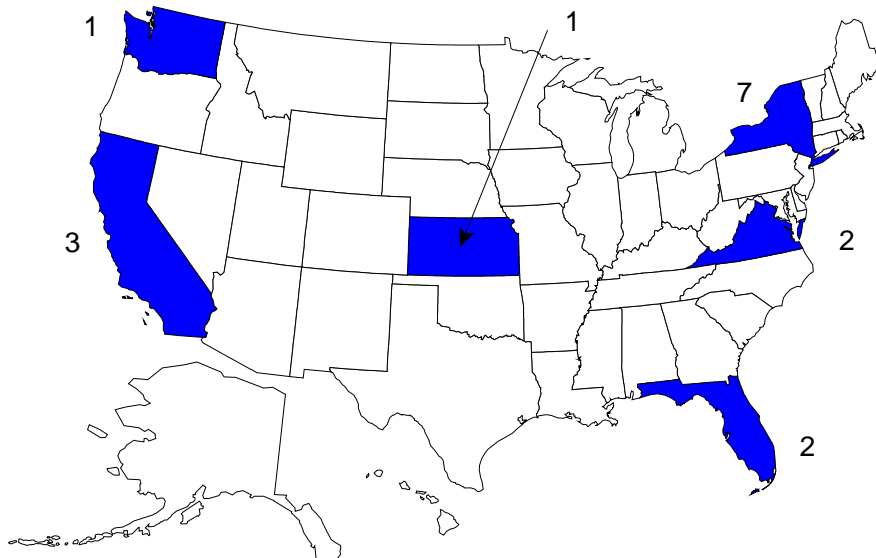
Usefulness of Information Provided by EPA and Others to Water Utilities

The survey shows that a variety of sources provided useful information to help water utilities prepare vulnerability assessments. Utilities cited consultants hired to assist in the preparation of vulnerability assessments most frequently as sources that provided useful information. Small utilities required to complete vulnerability assessments by June 30, 2004, may not be able to hire consultants and could be disadvantaged. Utilities also cited other sources – such as EPA, AWWA, Water-ISAC, and local law enforcement – as providing useful information. However, the survey results show that utilities did not always obtain information from all possible sources.

As we reported in *EPA Needs to Assess the Quality of Vulnerability Assessments Related to the Security of the Nation's Water Supply* (Report No. 2003-M-00013), dated September 24, 2003, vulnerability assessments follows a threat-driven process. EPA was responsible for providing adequate threat information to water utilities in order to prepare vulnerability assessments. EPA did this through a variety of methods. First, EPA provided $53 million toward grants to the largest water utilities. Utilities primarily used the grants to hire water security consultants to assist in conducting vulnerability assessments. EPA also provided $21 million in grants to provide drinking water security training to medium and small water utilities. Further, EPA utilized the Water-ISAC and the AWWA to provide threat information to water utilities. According to the Bioterrorism Act, however, the responsibility for determining which threats to protect against ultimately resides with each water utility.

We identified five key security activities or capabilities critiqued through the vulnerability assessment process.

- Threat Identification
- Detection
- Delay
- Response and Consequence
- Remote Access

Threat identification serves as the first step in the vulnerability assessment process. Threat information is necessary to identify potential scenarios against which utilities should prepare. For example, security preparations may differ for internal threats from disgruntled employees versus external threats from vandals or terrorists. The next step in the vulnerability assessment process determines how well a utility can detect a problem. This includes reviewing security and monitoring features; for example, how quickly a utility discovered a contaminant in the distribution system. The third step measures the delay system. This involves an examination of barriers such as gates, fences, locks, and walls. The next step measures response capabilities by reviewing the capacity of the water utility in conjunction with Federal, State, and local authorities to respond and neutralize the adversary. Another step for some utilities involves

examining the remote access system, commonly known as the SCADA system. This involves assessing the computer system to determine the ease at which someone could control the utility remotely.

The following sections provide detailed information from the survey results on the usefulness of the information provided to water utilities. Differences between the number of responses and total number of utilities indicate that some utilities did not receive information from that source. Two of the water utilities most frequently responded "not useful" or "not very useful" about the information they obtained from EPA and other sources.

Many Sources Provided Useful Threat Information

The survey shows that a variety of sources provided useful threat information to help water utilities prepare vulnerability assessments. The survey shows that respondents most frequently cited consultants hired by water utilities and EPA as providing useful threat information. Of the 16 water utilities surveyed, 13 responded favorably about information obtained from consultants they hired, including five utilities that described the information they received as "very useful." In addition, 12 of the 16 utilities responded that EPA provided useful threat information. According to respondents, other sources of useful threat information included the Water-ISAC, AWWA, water security experts, and local law enforcement agencies.

Figure 2: Satisfaction with Threat Information
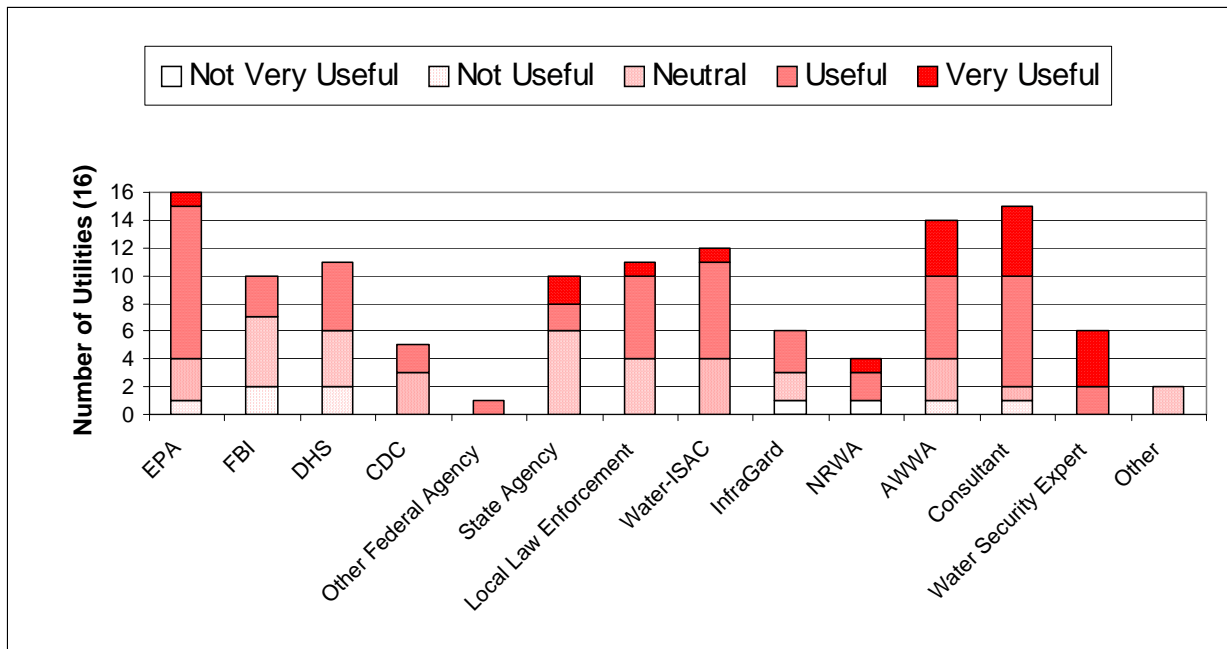
Consultants Provided Useful Detection Information

The survey responses show that, of the sources that provided detection information to water utilities, respondents most frequently cited consultants hired by water utilities as providing useful detection information. Of the 16 water utilities, 13 responded favorably about information obtained from consultants they hired, including five utilities that described the information they received as "very useful." In addition to consultants, the AWWA, local law enforcement, Water-ISAC, and EPA also provided useful detection information for five to seven of the utilities.

Figure 3: Satisfaction with Detection Information
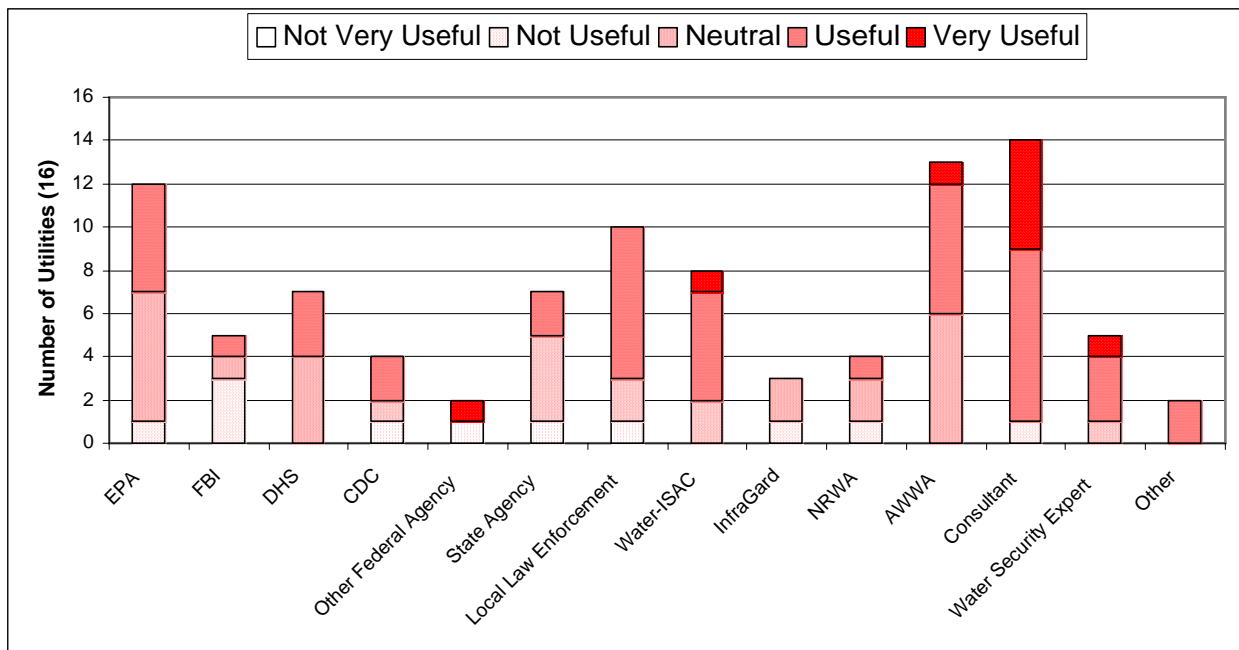
Consultants and the AWWA Provided Useful Delay Information

The survey responses show that, of the sources that provided delay information, respondents most frequently cited consultants hired by water utilities and the AWWA as providing useful delay information. Of the 16 surveys, 12 listed consultants hired by water utilities as having useful information, including six utilities who ranked the information as "very useful." In addition to consultants, 10 utilities listed AWWA as having provided useful delay information. Local law enforcement also provided useful delay information for six of the utilities.

Figure 4: Satisfaction with Delay Information
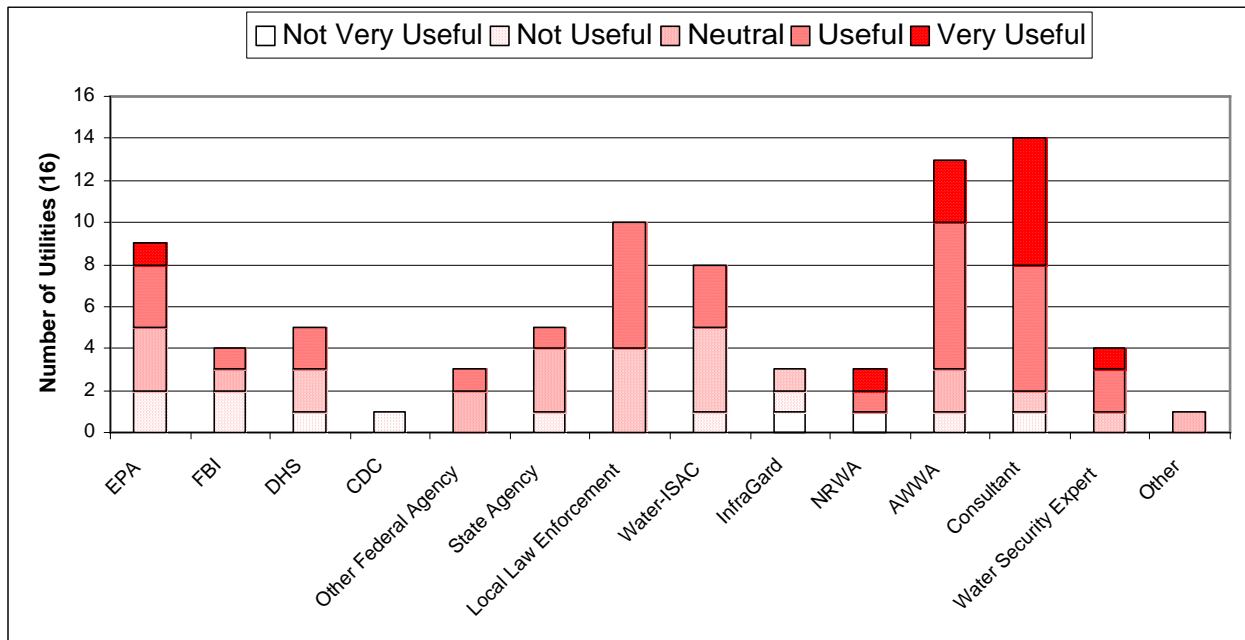
Consultants and the AWWA Provided Useful Response and Consequence Information

The survey responses show that, of the sources that provided response and consequence information, respondents most frequently cited consultants hired by water utilities and the AWWA as providing useful response and consequence information. Of the 16 surveys, 11 listed consultants hired by water utilities as having useful information, including five utilities who ranked the information as "very useful." In addition to consultants, nine utilities listed AWWA as providing useful response and consequence information. State agencies also provided useful response and consequence information for six of the utilities.

Figure 5: Satisfaction with Response and Consequence Information
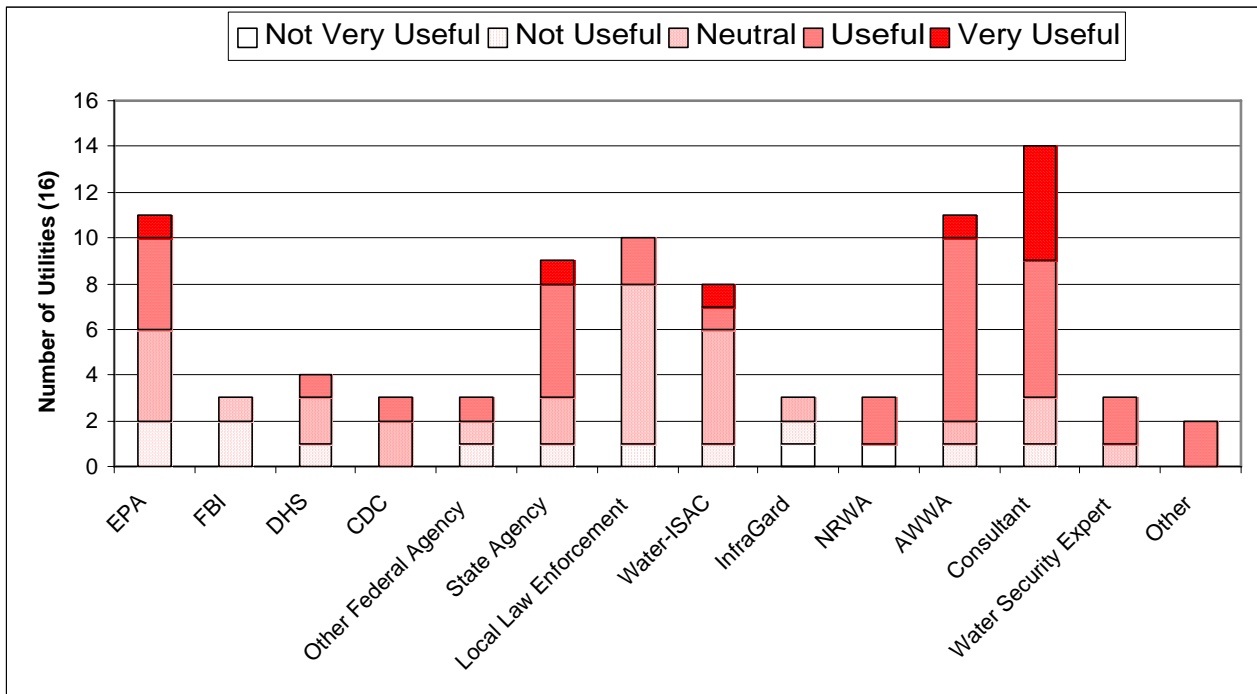
Consultants Provided Useful Remote Access Information

Many utilities use a remote access system, commonly known as SCADA, to control operations. The survey responses show that, of the sources that provided SCADA information, respondents most frequently cited consultants hired by water utilities as providing useful SCADA information. Of the 15 surveys,[7] 11 listed consultants hired by water utilities as having useful information, including three utilities who ranked the information as "very useful." In addition to consultants, six utilities listed AWWA and five utilities listed Water-ISAC as providing useful SCADA information.

Figure 6: Satisfaction with Remote Access Information

---
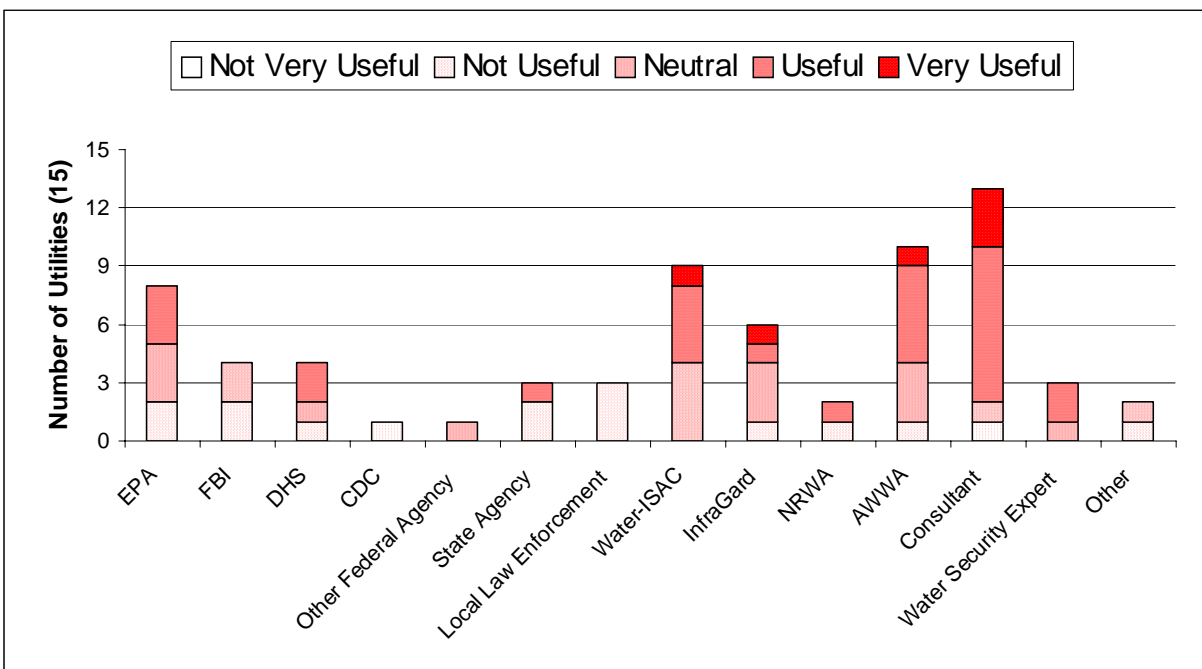
[7]One utility did not have a SCADA system.

Additional Security Concerns of Water Utilities

EPA's Strategic Plan for Homeland Security focuses on preparedness and prevention, assisting those responsible for critical infrastructures in assessing and reducing vulnerabilities and maximizing their response capabilities. EPA also intends to develop technologies to improve the Nation's critical infrastructure and key responders' abilities to detect and monitor environmental threats. The survey asked questions to help determine utilities' technological needs. All of the utilities surveyed had concerns for water security described in more detail below. The concerns include:

- additional information regarding vulnerabilities;
- financing security improvements;
- training assistance;
- research; and
- procedural changes.

Additional Information Needed by Utilities

The survey results show that water utilities still have a need for more information regarding threats, detection assistance, delay, response and consequence mitigation, and SCADA (see Figure 7).

Figure 7: Number of Utilities That Would Like Additional Information
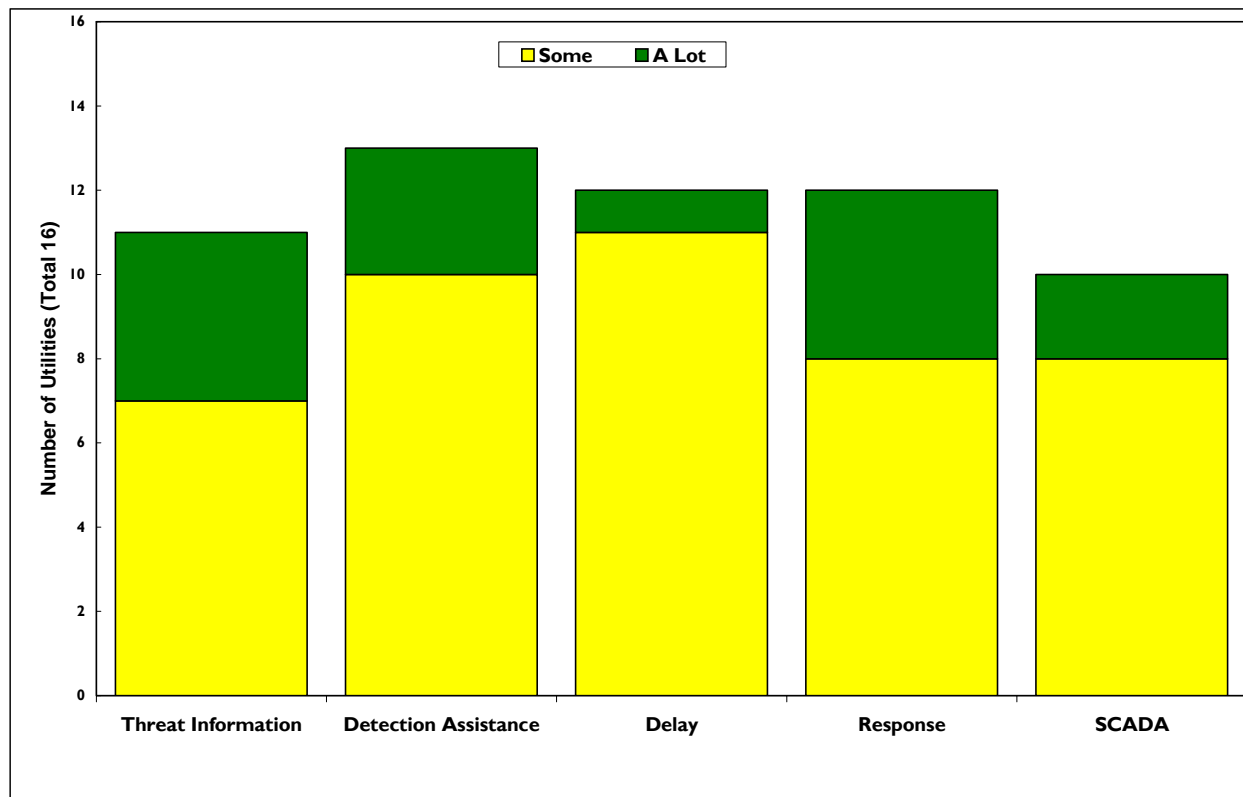
EPA funded the Water-ISAC to promote information sharing on water security. The Water-ISAC claims to provide information to water utilities that serve 80 percent of all drinking water customers. Five of the utilities in our survey, however, responded that they want better access to threat information, including access to the Water-ISAC database which is only available on a subscription fee basis. In addition, four utilities (including two medium sized utilities) did not obtain threat information from the Water-ISAC. We do not know why the utilities did not obtain threat information from the Water-ISAC.

Financial Assistance Needed by Utilities

Utilities stated that they need financial assistance to make necessary security improvements. Of the 16 utilities, 11 estimated that they would spend more than $100,000 during the next 12 months on water security improvements, including four utilities who plan to spend more than $1 million (see Figure 8).

Figure 8: Amount of Money Water Utilities Expect to Spend in the Next 12 Months on Security Improvements
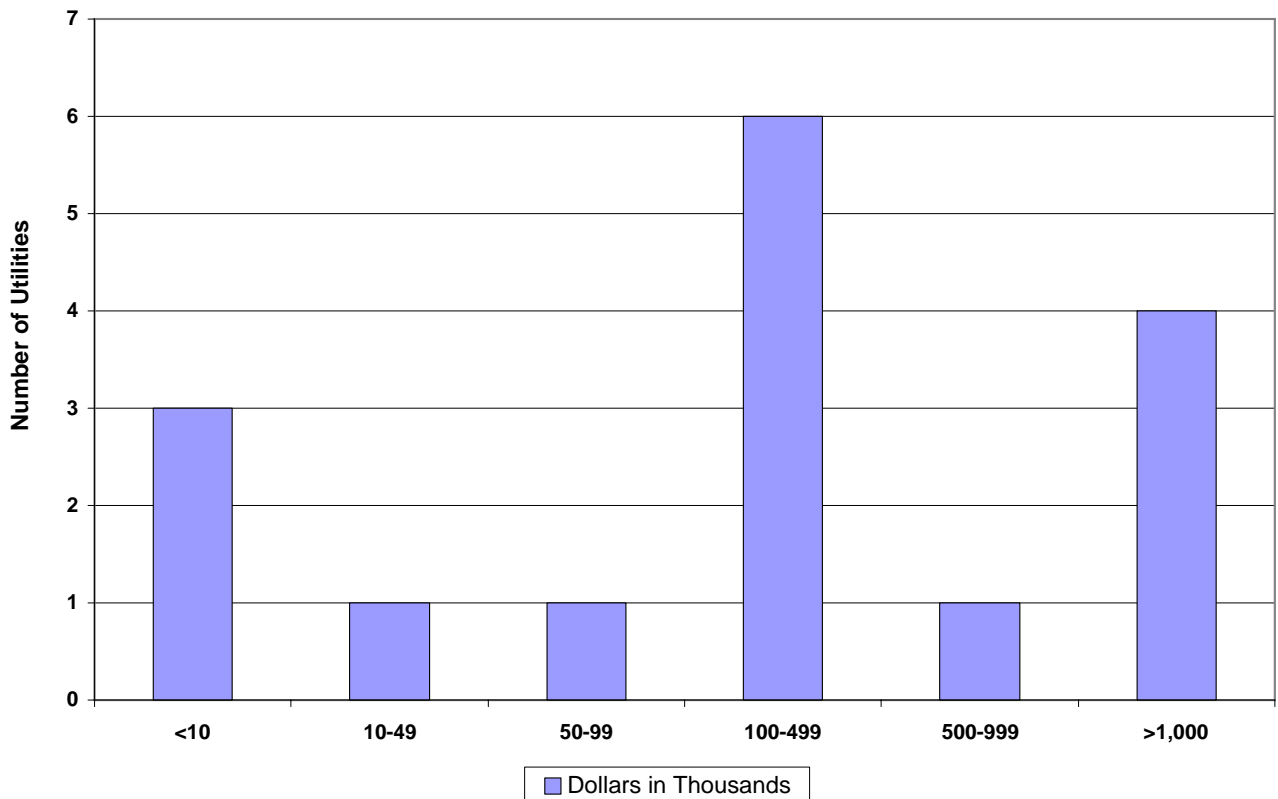
Of the 16 utilities, 11 stated that they may limit security improvements to those that they can afford and/or budget as capital improvement projects. Several utilities stated that they would issue bonds or raise water rates to cover the costs of security improvements (see Figure 9).

Figure 9: How Water Utilities Plan to Pay for Security Improvements[8]
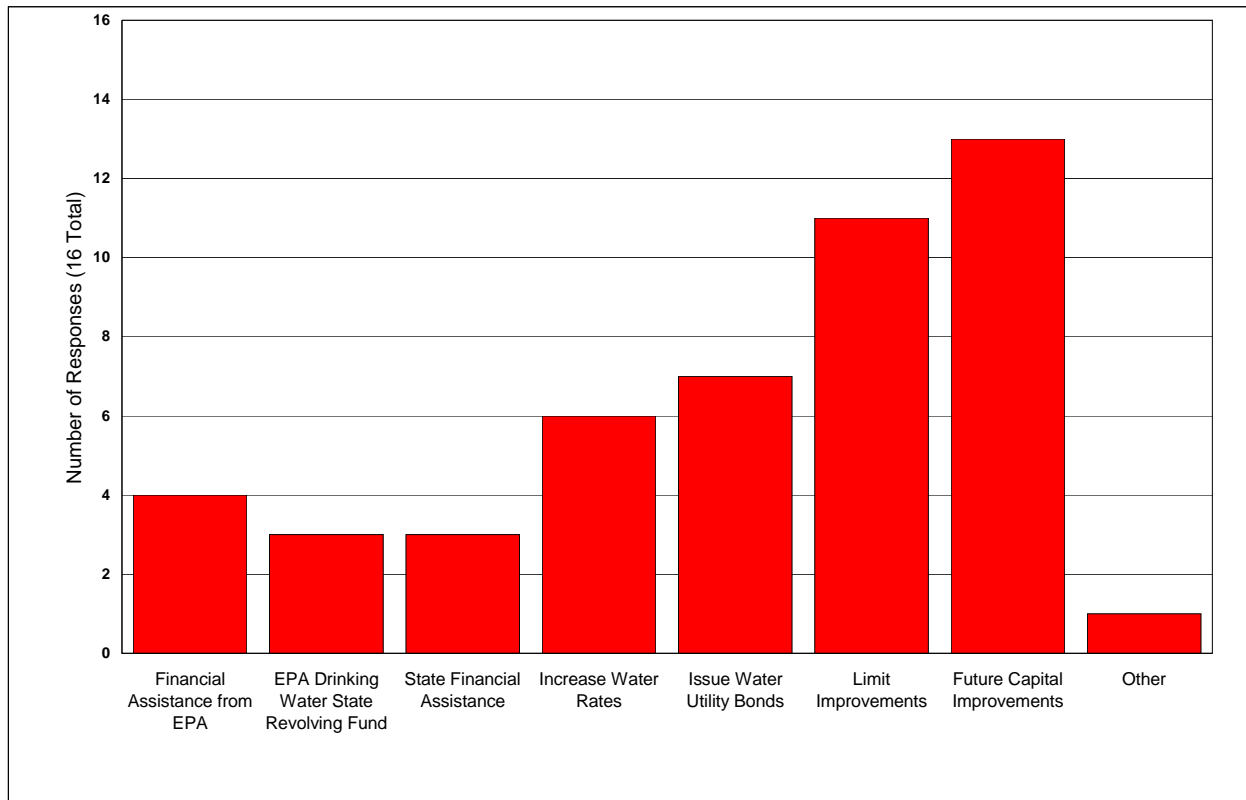
Seven of the 16 utilities responded that they needed financial assistance. EPA has limited its financial assistance to ensuring that drinking water utilities receive technical assistance and training on vulnerability assessments and emergency response plans, but not funding for the improvements themselves. Three utilities indicated that they plan to use EPA's Drinking Water State Revolving Fund to help pay for security improvements. The survey results do not indicate whether the 13 utilities who do not plan on using the Drinking Water State Revolving Fund realize that they can use the fund to provide assistance for implementing infrastructure-related security measures.

---

[8]The survey allowed respondents to check more than one answer.

Training Needs

Of the 16 utilities, 14 described additional training that their employees needed to improve security. The training needs ranged from general seminars on security awareness to specific training such as crime scene preservation. Of the 16 utilities, 14 stated that they needed additional training in emergency response, including identifying and detecting threats. Four of the utilities stated that they wanted to conduct training exercises or drills to help them prepare for actual security events.

Research Needs

Twelve utilities stated that they would like EPA to fund research on monitoring and detecting contaminants. The utilities stated that they would like to have real-time monitoring of water systems to detect chemical and biological agents, particularly in the distribution system, which many experts view as the most susceptible to terrorist attack. One utility indicated that they wanted EPA to provide rapid response lab analysis and sampling capabilities.

Procedural Changes Needed

Eight survey respondents stated that they would like to see specific procedural changes made to improve security, while six stated that they did not want any changes. Since no consensus emerged about changes needed, the following list reflects the respondents' suggestions, including those that would likely be addressed by State or local authorities:

- Include security practices as part of water operations certification training.
- Provide a time frame for renewing vulnerability assessments.
- Change the rules governing the awarding and uses of Drinking Water State Revolving Fund loans and grants.
- Establish security standards for water utilities.
- Modify the Freedom of Information Act to protect sensitive information about water facilities.
- Improve the ability to conduct background checks on employees.
- Provide additional State police to respond to malevolent acts.

Performance Indicators that EPA Could Use to Measure Improvements in Water Security Levels

In our report *EPA Needs a Better Strategy to Measure Changes in the Security of the Nation's Water Infrastructure* (Report No. 2003-M-00016), dated September 11, 2003, we suggested that EPA develop performance indicators to measure changes in water security. EPA stated that they would welcome recommendations and assistance in this area. In our survey, we asked water utilities to respond to questions about performance indicators that could be used to measure changes in water security. We used the input from the survey to develop the following performance indicators which could be used to measure changes in water security levels.

Length of time a water utility could provide water during or after a security incident

> Eleven of the utilities mentioned this type of performance indicator. This indicator would incorporate improvements made by water utilities such as adding storage facilities, interconnections, and emergency backup power sources.

Detection and response times

> Twelve utilities mentioned this type of performance indicator. Water utilities could perform exercises with a variety of threat scenarios to determine the length of time to detect and respond to threats. Utilities could also use the drills to determine whether employees utilized appropriate response procedures.

Ability to detect contaminants in water system

> Ten utilities mentioned this type of performance indicator. Detection is critical for a water utility to adequately respond to threats. Utilities also suggested measuring the number of contaminants or the timeliness of detecting particular contaminants in the water system. Tests could also monitor the timeliness of the laboratory used by the utility to identify contaminants.

Ability to detect attempted intrusions into the SCADA system

> Seven utilities mentioned this type of performance indicator. Water utilities could document the number of attempted intrusions into their SCADA systems to track the level of interest in the water system.

Suggestions

Based on the survey results and our observations, we offer the following suggestions:

(1) Ensure that small utilities have access to security information that large utilities received from consultants funded by EPA, possibly by fully funding the Water-ISAC, and provide lists of other agencies from which utilities could obtain information.

(2) Ensure that water utilities have access to information on funding security enhancements, including use of the Drinking Water State Revolving Fund.

(3) Consider using the performance indicators discussed above to set a baseline for water security and measure improvements over time, particularly through the use of exercises and drills to test the security of water utilities.

The following series of questions deal with information or guidance the drinking water utility received, and its usefulness in preparing for a vulnerability assessment.

1. **Threats** – In order to conduct a vulnerability assessment, a utility needs to determine or evaluate potential threats, often referred to as a design basis threat. The design basis threat is based on understanding the motives, intentions, and capabilities of the utility's adversaries.

    Below are a list of sources from which your drinking water utility may have received information or guidance on **THREATS**. Please rate the usefulness of the information you received on a scale from one to five, where one is not at all useful and five is very useful. If you did not receive information from a listed source, please check that box.

Sources of Threat Information (check all that apply)	Not useful				Very useful	Did not receive information
	1*	2	3	4	5*	
Environmental Protection Agency (EPA)						
Federal Bureau of Investigation (FBI)						
Department of Homeland Security						
Centers for Disease Control (CDC)						
Other Federal agency Please specify_____						
State agency Please specify _____						
Local law enforcement (Police, Sheriff)						
Water Information Sharing and Analysis Center (Water-ISAC)						
InfraGard						
National Rural Water Association (NRWA)						
American Water Works Association (AWWA)						
Consultant hired to prepare vulnerability assessment						
Water security expert						
Other – Please specify _____						

* provide explanation for answers with either 1 (not at all useful) or 5 (very useful)

2. **Detection** – Detection (1) senses an act of aggression, (2) assesses the validity of the detection, and (3) communicates the appropriate information to a response force. A detection system must provide all three of these capabilities to be effective. A detection system may consist of closed-circuit television, cameras, motion sensors, alarms, door or window sensors, and chemical and biological monitoring and detection technologies.

   Below are a list of sources from which your drinking water utility may have received information or guidance on **DETECTION**. Please rate the usefulness of the information you received on a scale from one to five, where one is not at all useful and five is very useful. If you did not receive information from a listed source, please check that box.

Sources of Detection Information (check all that apply)	Not useful			Very useful		Did not receive information
	1*	2	3	4	5*	
Environmental Protection Agency (EPA)						
Federal Bureau of Investigation (FBI)						
Department of Homeland Security						
Centers for Disease Control (CDC)						
Other Federal agency Please specify_____						
State agency Please specify _____						
Local law enforcement (Police, Sheriff)						
Water Information Sharing and Analysis Center (Water-ISAC)						
InfraGard						
National Rural Water Association (NRWA)						
American Water Works Association (AWWA)						
Consultant hired to prepare vulnerability assessment						
Water security expert						
Other – Please specify _____						

* **provide explanation for answers with either 1 (not at all useful) or 5 (very useful)**

3. **Delay** – Delay is any mechanisms in place to delay the intruder, after detection, from damaging the utility or contaminating the water. Defensive measures protect an asset by delaying an adversary's movement toward the asset or by shielding the water from contamination. Delay measures include such things as fencing, locks, and grates or bars on windows.

Below are a list of sources from which your drinking water utility may have received information or guidance on **DELAY**. Please rate the usefulness of the information you received on a scale from one to five, where one is not at all useful and five is very useful. If you did not receive information from a listed source, please check that box.

Sources of Delay Information (check all that apply)	Not useful			Very useful		Did not receive information
	1*	2	3	4	5*	
Environmental Protection Agency (EPA)						
Federal Bureau of Investigation (FBI)						
Department of Homeland Security						
Centers for Disease Control (CDC)						
Other Federal agency Please specify_____						
State agency Please specify _____						
Local law enforcement (Police, Sheriff)						
Water Information Sharing and Analysis Center (Water-ISAC)						
InfraGard						
National Rural Water Association (NRWA)						
American Water Works Association (AWWA)						
Consultant hired to prepare vulnerability assessment						
Water security expert						
Other – Please specify _____						

* **provide explanation for answers with either 1 (not at all useful) or 5 (very useful)**

4. **Response/Consequence Mitigation –** Consequences are outcomes that can happen if an adversary successfully carries out a threat. Consequences of a threat carried out on a water supply can affect the quantity and/or quality of water supplied, as well as general sanitation and safety issues in a community.

Below are a list of sources from which your drinking water utility may have received information or guidance on **RESPONSE/CONSEQUENCE MITIGATION**. Please rate the usefulness of the information you received on a scale from one to five, where one is not at all useful and five is very useful. If you did not receive information from a listed source, please check that box.

Sources of Response/Consequence Mitigation Information (check all that apply)	Not useful			Very useful		Did not receive information
	1*	2	3	4	5*	
Environmental Protection Agency (EPA)						
Federal Bureau of Investigation (FBI)						
Department of Homeland Security						
Centers for Disease Control (CDC)						
Other Federal agency Please specify_____						
State agency Please specify _____						
Local law enforcement (Police, Sheriff)						
Water Information Sharing and Analysis Center (Water-ISAC)						
InfraGard						
National Rural Water Association (NRWA)						
American Water Works Association (AWWA)						
Consultant hired to prepare vulnerability assessment						
Water security expert						
Other – Please specify _____						

* **provide explanation for answers with either 1 (not at all useful) or 5 (very useful)**

20

5. **Cyber** – Water utility components are often controlled remotely by computer systems called Supervisory Control and Data Acquisition (SCADA). These SCADA systems are susceptible to attack by computer hackers who could shut down critical assets within the water utility.

Below are a list of sources from which your drinking water utility may have received information or guidance on **<u>SCADA SECURITY</u>**. Please rate the usefulness of the information you received on a scale from one to five, where one is not at all useful and five is very useful. If you did not receive information from a listed source, please check that box.

Sources of SCADA Security Information (check all that apply)	Not useful				Very useful	Did not receive information
	1*	2	3	4	5*	
Environmental Protection Agency (EPA)						
Federal Bureau of Investigation (FBI)						
Department of Homeland Security						
Centers for Disease Control (CDC)						
Other Federal agency Please specify_____						
State agency Please specify _____						
Local law enforcement (Police, Sheriff)						
Water Information Sharing and Analysis Center (Water-ISAC)						
InfraGard						
National Rural Water Association (NRWA)						
American Water Works Association (AWWA)						
Consultant hired to prepare vulnerability assessment						
Water security expert						
Other – Please specify _____						

* **provide explanation for answers with either 1 (not at all useful) or 5 (very useful)**

Performance Measurement Information

6. What performance indicators would best measure changes in the overall level of water security? (Some examples may include: length of time your water utility could supply water in the event of a disaster, length of time your water utility could operate on emergency backup power sources, amount of water storage your utility has).

    _____

    _____

    _____

7. Should there be separate performance indicators that would measure changes for each component of the water utility (source water, treatment, storage, distribution)? What performance indicators would best measure these changes?

    _____

    _____

    _____

8. What performance indicators would best measure changes in threat detection? (Some examples may include: number of contaminants your water utility can detect in the distribution system, amount of time it takes to determine whether a detection event is a real threat or false alarm).

    _____

    _____

    _____

9. What performance indicators would best measure changes in adversary delay? (An example may include: amount of time the utility can delay threats compared to response time).

    _____

    _____

    _____

10. What performance indicators would best measure changes in response/consequence mitigation? (An example may include: number of employees that follow the proper response to specific threat scenarios in practice exercises)?

_____

_____

_____

11. What performance indicators would best measure changes in SCADA security systems? (An example may include: the number of attempts to hack into the system).

_____

_____

_____

Resource/Training Needs

12. How much money does your utility expect to spend on security enhancements over the next 12 months?
    ____ < $10,000
    ____ $10,000 - $50,000
    ____ $50,000 - $100,000
    ____ $100,000 - $500,000
    ____ $500,000 - $1,000,000
    ____ $1,000,000+
    ____ Don't know

13. By what means is your utility planning to pay for needed security enhancements?

		Yes	No	Don't Know
a.	Financial assistance from EPA	1	2	3
b.	EPA State Revolving Fund	1	2	3
c.	Financial assistance from the State	1	2	3
d.	Increase water rates	1	2	3
e.	Issue water utility bonds	1	2	3
f.	Limit improvements to those which the utility can afford	1	2	3
g.	Budget for future Capitol Improvement projects	1	2	3
h.	Other	1	2	3
	(Please specify _____)			

14. In which of the following areas do you need more assistance (check all that apply)?

		Little	Some	A Lot
a.	Threat information	1	2	3
b.	Detection assistance	1	2	3
c.	Delay	1	2	3
d.	Response	1	2	3
e.	SCADA	1	2	3

15. What specific assistance do you need (if any)?

_____

_____

16. Please describe the kinds of training employees at your facility need to improve security or response?

_____

_____

_____

17. What kinds of regulatory changes (if any) does your utility need to help improve security?

_____

_____

_____

18. What types of research (if any) would be most beneficial to improve security?

_____

_____

_____

19. Do you have any additional comments or concerns regarding water security?

_____

_____

Background Information

Utility Name: _____

20. What is the population served by your utility?

        ____Less than 3,300
        ____3,300 - 50,000
        ____50,000 - 100,000
        ____100,000 - 1,000,000
        ____1,000,000 - 3,000,000
        ____3,000,000+

21. Who performed the vulnerability assessment at your utility (check all that apply)?

        _____A consultant with expertise preparing a vulnerability assessment
        _____A security expert employed by the utility
        _____Other utility employee - please specify employee's title _____
        _____Someone else - please specify _____
        _____Don't know

22. Please indicate your utility's current status in:

		Planning	Conducting	Completed
a.	Vulnerability assessment	1	2	3
b.	Emergency response plan	1	2	3
c.	Implementing security improvements	1	2	3

23. What tools and methods were used to conduct your drinking water utility's vulnerability assessment (check all that apply)?

        _____Risk Assessment Methodology-Water (RAM-W)
        _____Vulnerability Self Assessment Tool (VSAT) software
        _____National Rural Water Association (NRWA) checklist
        _____Other - please specify_____
        _____Don't know

THANK YOU FOR YOUR ASSISTANCE IN COMPLETING THIS SURVEY.

Distribution

EPA Headquarters

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

EPA Office of Inspector General

Inspector General (2410)
Assistant Inspector General for Program Evaluation
Assistant Inspector General for Audit
Assistant Inspector General for Human Capital
Assistant Inspector General for Planning, Analysis and Results
Assistant Inspector General for Congressional and Public Liaison
Counsel