EPA United States Environmental Protection Agency

Office of Water (4601M)
EPA 817-K-06-001
www.epa.gov/watersecurity
February 2006

Recycled/Recyclable • Printed with Vegetable Oil Based Inks on 100% Postconsumer, Process Chlorine Free Recycled Paper

EPA
United States
Environmental Protection
Agency

Office of Water (4601M)
EPA 817-K-06-001
www.epa.gov/watersecurity
February 2006

B. National Measures

The NDWAC recommended that EPA consider three potential measures of national, sector-wide, aggregate progress:

- Implementation of active and effective security programs as measured by the degree of implementation of the 14 program features and corresponding feature-specific measures.
- Reduction in security risks as measured by the total number of assets determined to be a high security risk and the number of former high security risk assets lowered to medium or low risk, based on the results of vulnerability assessments.
- Reduction in the inherent risk potential of utility operations as measured by Clean Air Act Section 112(r) reporting on hazardous substances and by the number of utilities that convert from use of gaseous chlorine to other forms of chlorine or other treatment methods.

With respect to a national measurement process, the NDWAC recommended that:

- Participation be voluntary;
- Results of national aggregate measures be presented only in aggregated form; and
- Issues associated with the need for data confidentiality (if any) be fully addressed before any national measurement program is put in place.

V. Conclusion

Ultimately, the goal of implementing the 14 security features recommended by NDWAC is to create a significant improvement in water security on a national scale, by reducing vulnerabilities, and therefore risk to public health from terrorist attacks and natural disasters. To create a sustainable effect, the sector as a whole must not only adopt and actively practice the features, but also incorporate the features into "business as usual."

Active and Effective Water Security Programs

National Drinking Water Advisory Council Recommendations on Water Security

SUMMARY REPORT

Table of Contents

Summary Report

This document provides a summary of the water security recommendations of the National Drinking Water Advisory Council (NDWAC). The purpose of this summary is to raise awareness of active and effective security features, resources, incentives, and measures for drinking water and wastewater utilities nationwide. EPA will supplement the NDWAC recommendations with additional implementation guidance. The full text of the NDWAC Report is available at www.epa.gov/safewater/ndwac/council.html. Readers are encouraged to go beyond this summary to the full NDWAC Report to understand the depth and context of their deliberations and recommendations.

I. How These Recommendations Were Developed

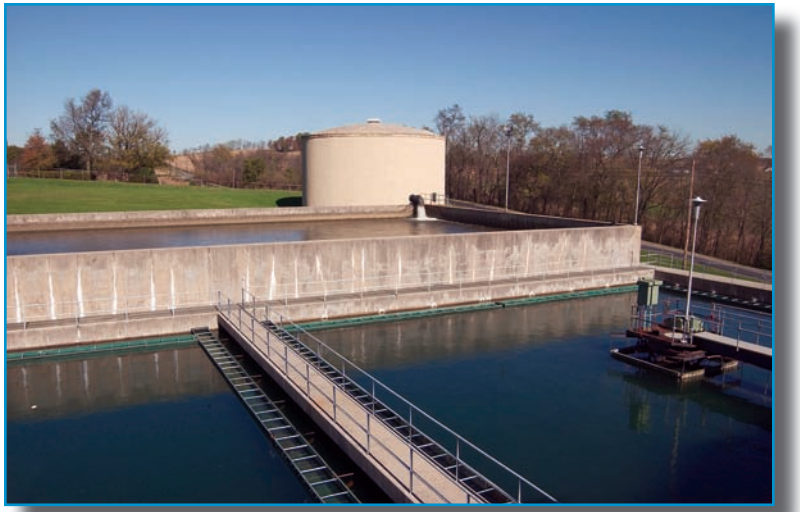
A secure water sector is critical to protect public health and ensure public confidence. In fall 2003, the NDWAC established a Water Security Working Group (WSWG) to consider and make recommendations on water security issues. The NDWAC directed the WSWG to:

- Identify active and effective security practices for drinking water and wastewater utilities, and provide an approach for adopting these practices.
- Recommend mechanisms to provide incentives that facilitate broad and receptive response among the water sector to implement active and effective security practices.
- Recommend mechanisms to measure progress and achievements in implementing active and effective security practices, and identify barriers to implementation.

The WSWG included stakeholders from many perspectives and used a collaborative, problem-solving approach to develop its findings, as illustrated in Figure 1. The WSWG presented its findings to the NDWAC, which unanimously adopted the findings as Council recommendations. The NDWAC recommendations on security are structured to maximize benefits to utilities by emphasizing actions that have the potential both to improve the quality or reliability of utility service, and to enhance security. The recommendations were designed for use by water systems of all types and sizes, including small systems.

Features	Potential Measures of Progress (see the full NDWAC report for all measures)	
Organizational Features		
Feature 1 - Explicit commitment to security	Does a written, enterprise-wide security policy exist, and is the policy reviewed regularly and updated as needed?	✓
Feature 2 - Promote security awareness	Are incidents reported in a timely way and reviewed, and are lessons learned from incident responses incorporated, as appropriate, into future utility security efforts?	✓
Feature 5 - Defined security roles and employee expectations	Are managers and employees who are responsible for security identified?	✓
Operational Features		
Feature 3 - Vulnerability assessment up to date	Are reassessments of vulnerabilities made after incidents, and are lessons learned and other relevant information incorporated into security practices?	✓
Feature 4 - Security resources and implementation priorities	Are security priorities clearly identified and to what extent do security priorities have resources assigned them?	✓
Feature 7 - Contamination detection	Is there a protocol/procedure in place to identify and respond to suspected contamination events?	✓
Feature 10 - Threat-level based protocols	Is there a protocol/procedure for responses to threat level changes?	✓
Feature 11 - Emergency Response Plan tested and up to date	Do exercises address the full range of threats - physical, cyber, and contamination - and is there protocol/procedure to incorporate lessons learned from exercises and actual responses into updated emergency response and recovery plans?	✓
Feature 14 - Utility-specific measures and self assessment	Does the utility perform self-assessment at least annually?	✓
Infrastructure Features		
Feature 6 - Intrusion detection and access control	To what extent are methods to control access to sensitive assets in place?	✓
Feature 8 - Information protection and continuity	Is there a procedure to identify and control security-sensitive information, is information correctly categorized, and how do control measures perform under testing?	✓
Feature 9 - Design and construction standards	Is there a protocol/procedure for incorporation of security considerations into internal utility design construction standards for new facilities/infrastructure and major maintenance projects?	✓
External Features		
Feature 12 - Communications	Is there a mechanism for utility employees, partners, and the community to notify the utility of suspicious occurrences and other security concerns?	✓
Feature 13 - Partnerships	Have reliable and collaborative partnerships with customers, managers of independent interrelated infrastructure, public health officials and providers, response organizations and other utilities been established?	✓

Table 1. Recommended measures to assess effectiveness of a utility's security program



IV. Measures to Assess Improvements in Security Programs

The main outcome of an active and effective security program is to ensure reliable operation of water and wastewater systems in times of crisis or disaster. Utilities should assess and seek to improve their security programs on an ongoing basis to keep programs "fresh," and take advantage of emerging approaches and new technologies. Assessment will increase the effectiveness and efficiency of security programs and organizations over time.

To aid utilities in identifying progress in improving security programs, the NDWAC recommended both utility-specific measures of security activities and achievements as well as suggesting national, sector-wide, aggregate measures of progress.

A. Utility-specific Measures

The NDWAC recommended measures of progress for security activities and achievements that should form the basis of a utility-specific self-assessment and measurement program. These measures could be considered by a full range of utilities, regardless of utility size, circumstance, or operating conditions. Each measure corresponds to one of the recommended features of an active and effective security program. Utilities could adapt or supplement the measures listed in Table 1 with additional measures that reflect the specific security approaches and tactics they have chosen. Additionally, other measures may be more appropriate for individual utilities.

The NDWAC identified 14 features of active and effective security programs that are important to increasing security and relevant across the broad range of utility circumstances and operating conditions. The 14 features are, in many cases, consistent with the steps needed to maintain technical, management, and operational performance capacity related to overall water quality. Many utilities may be able to adopt some of the features with minimal, if any, capital investment.

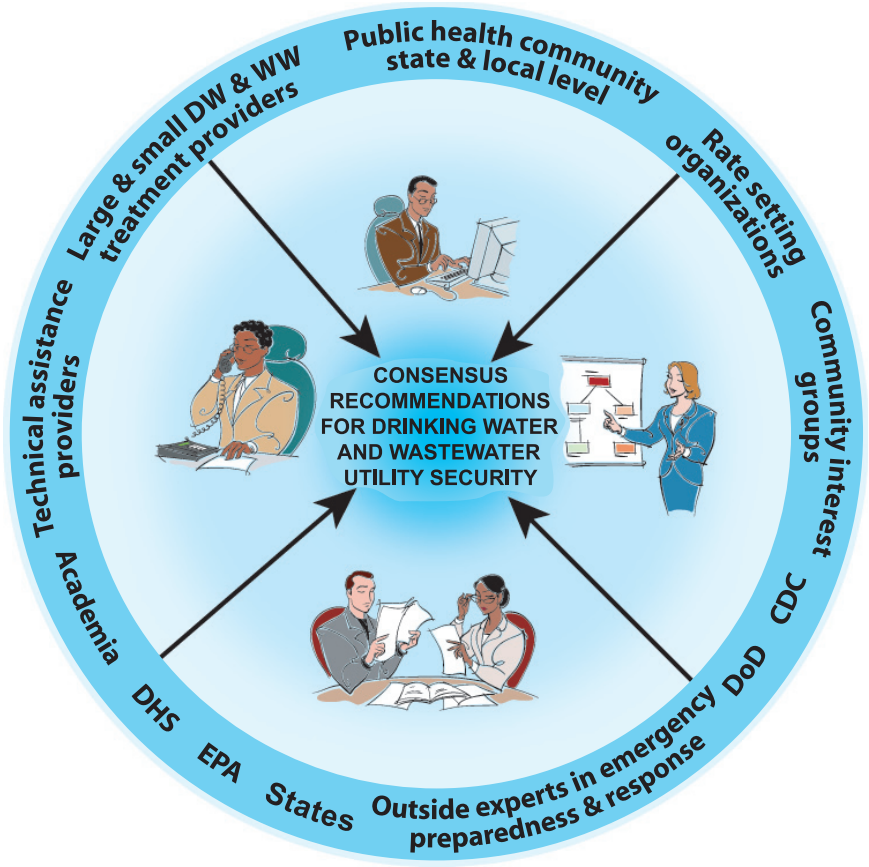


Figure 1. A variety of stakeholders worked together collaboratively to arrive at recommendations that can be used by all utilities

II. Features Of An Active And Effective Security Program

The centerpiece of the NDWAC's recommendations defines an "active and effective" utility security program. In identifying common features of active and effective security programs, the NDWAC emphasized that "one size does not fit all" and that there will be variability in security approaches and tactics among water utilities, based on utility-specific circumstances and operating conditions. The 14 features:

- Are sufficiently flexible to apply to all utilities, regardless of size.
- Incorporate the idea that active and effective security programs should have measurable goals and time lines.
- Allow flexibility for utilities to develop specific security approaches and tactics that are appropriate to utility-specific circumstances.

Water utilities can differ in many ways including:

- Supply source (ground water, surface water, etc.)
- Number of supply sources
- Treatment capacity
- Operational risk
- Location risk
- Security budget
- Spending priorities
- Political and public support
- Legal barriers
- Public vs. private ownership

The NDWAC recommends that all utilities address security in an informed and systematic way, regardless of these differences. Utilities need to fully understand the specific, local circumstances and conditions under which they operate, and develop a security program tailored to those conditions. The NDWAC's goal in identifying common features of active and effective security programs is to achieve consistency in security program outcomes among water utilities, while allowing for and encouraging utilities to develop utility-specific security approaches and tactics. The features are based on an integrated approach that incorporates a combination of public involvement and awareness, partnerships, and physical, chemical, operational, and design controls to increase overall program performance. They address utility security in four functional categories: *organizational, operational, infrastructure,* and *external*. Figure 2 illustrates the features and their functional categories.

III. Incentives for Utilities to Develop an Active and Effective Security Program

To provide recognition and incentives that facilitate receptiveness among the water sector to implement active and effective security programs, the NDWAC recommended that EPA, DHS, state agencies, and water and wastewater utility organizations:

- Provide information on the importance of active and effective security programs to utilities, to communicate to owners and operators the benefits of active and effective security programs and the potential negative consequences of failing to address security.
- Develop programs and/or awards that recognize utilities that develop and maintain active and effective security programs, and that demonstrate superior security performance.
- Support development and implementation of a voluntary utility security peer technical assistance and review program.
- Help utilities develop active and effective security programs by providing different types of technical assistance, including technology verification information.
- Support utility security programs by helping utilities obtain access to needed security-related support systems and infrastructure, and by supporting inclusion of utilities in security exercises.
- Support security enhancements with grant and loan programs focused on security, without reducing existing non-security focused grant and loan programs.
- Provide educational and other materials to boards, utility governing bodies, and rate setting organizations to help them understand costs associated with implementing active and effective security programs.

understanding and to share information about the utility's security concerns and planning. Such efforts will maximize the efficiency and effectiveness of a mutual aid program during an emergency response effort, as the organizations will be familiar with each others' circumstances, and thus will be better able to serve each other.

It is also important for utilities to develop partnerships with the communities and customers they serve. Partnerships help to build credibility within communities and establish public confidence in utility operations. People who live near utility structures ("water watchers") can be the eyes and ears of the utility, and can be encouraged to notice and report changes in operating procedures or other suspicious behaviors.

Utilities and public health organizations should establish formal agreements on coordination to ensure regular exchange of information between utilities and public health organizations, and outline roles and responsibilities during response to and recovery from an emergency. Coordination is important at all levels of the public health community—national public health, county health agencies, and health-care providers, such as hospitals.

Feature 13 Resources

Security Information Collaboratives Guide
www.epa.gov/nhsrc/pubs/brochureSIC051805.pdf
Domestic Terrorism: Resources for Local Government
www.nlc.org/Issues/Homeland_Security___Public_Safety/index.cfm
Florida's Water-Wastewater Agency Response Network (FlaWARN)
www.flawarn.org

Figure 2. The 14 features of an active and effective security program

A. Organizational Features

There is always something that can be done to improve security. Even when resources are limited, the simple act of increasing organizational attentiveness to security may reduce vulnerability and increase preparedness. The first step to achieving preparedness is to make security a part of the organizational culture, so that it is in the day-to-day thinking of front-line employees, emergency responders, and management of every water and wastewater utility in a community. To successfully incorporate security into "business as usual," there must be a strong commitment to security by organization leadership and by the supervising body, such as the utility board or rate setting organization. The following features address how a security culture can be incorporated into an organization.

Feature 1. Make an explicit and visible commitment of the senior leadership to security.

Utilities should create an explicit, visible, easily communicated, enterprise-wide commitment to security, which can be done through:

- Incorporating security into a utility-wide mission or vision statement, addressing the full scope of an active and effective security program—that is, protection of public health, public safety, and public confidence, and that is part of core day-to-day operations.
- Developing an enterprise-wide security policy or set of policies.

Utilities should use the process of making a commitment to security as an opportunity to raise awareness of security throughout the organization, making the commitment visible to all employees and customers, and to help every facet of the enterprise recognize the contribution they can make to enhancing security.

Feature 1 Resource
Establishing the Security Culture Begins from the Top
www.cisco.com/web/about/security/intelligence/05_07_security-culture.html

Feature 2. Promote security awareness throughout the organization.

The objective of a security culture should be to make security awareness a normal, accepted part of day-to-day operations. Examples of tangible efforts include:

- Conducting employee training;
- Incorporating security into job descriptions;
- Establishing performance standards and evaluations for security;
- Creating and maintaining a security tip line and suggestion box for employees;
- Making security a routine part of staff meetings and organization planning, and
- Creating a security policy.

Feature 2 Resource
Water Security Training Courses, Meetings, and Workshops/ Webcasts, USEPA
cfpub.epa.gov/safewater/watersecurity/outreach.cfm

D. External Features

Strong relationships with response partners and the public strengthen security and public confidence. Two of the recommended features of active and effective security programs address this need.

Feature 12. Develop and implement strategies for regular, ongoing security-related communications with employees, response organizations, rate setting organizations, and customers.

An active and effective security program should address protection of public health, public safety (including infrastructure), and public confidence. Utilities should create an awareness of security and an understanding of the rationale for their overall security management approach in the communities they serve, including rate setting organizations.

Effective communication strategies consider key messages; who is best equipped/trusted to deliver the key messages; the need for message consistency, particularly during an emergency; and the best mechanisms for delivering messages and for receiving information and feedback from key partners. The key audiences for communication strategies are utility employees, response organizations, and customers.

Feature 12 Resource
Security Risk Communication Training
www.epa.gov/safewater/dwa/course-genint.html

Feature 13. Forge reliable and collaborative partnerships with the communities served, managers of critical interdependent infrastructure, response organizations, and other local utilities.

Effective partnerships build collaborative working relationships and clearly define roles and responsibilities, so that people can work together seamlessly if an emergency should occur. It is important for utilities within a region and neighboring regions to collaborate and establish a mutual aid program with neighboring utilities, response organizations, and sectors, such as the power sector, on which utilities rely or impact. Mutual aid agreements provide for help from other organizations that is prearranged and can be accessed quickly and efficiently in the event of a terrorist attack or natural disaster. Developing reliable and collaborative partnerships involves reaching out to managers and key staff in other organizations to build reciprocal

Feature 9. Incorporate security considerations into decisions about acquisition, repair, major maintenance, and replacement of physical infrastructure; include consideration of opportunities to reduce risk through physical hardening and adoption of inherently lower-risk design and technology options.

Prevention is a key aspect of enhancing security. Consequently, consideration of security issues should begin as early as possible in facility construction (i.e., it should be a factor in facility plans and designs). However, to incorporate security considerations into design choices, utilities need information about the types of security design approaches and equipment that are available and the performance of these designs and equipment in multiple dimensions. For example, utilities would evaluate not just the way that a particular design might contribute to security, but also would look at how that design would affect the efficiency of day-to-day plant operations and worker safety. Numerous resources are available to provide information for designers and owners/operators of water utilities on design approaches and upgrades that improve security and reduce vulnerability.

Feature 9 Resources

EPA Security Product Guides
epa.gov/watersecurity/guide

Interim Voluntary Security Guidelines for Water Utilities (2004), issued by AWWA under a grant from EPA
www.awwa.org/science/wise

Interim Voluntary Security Guidance for Wastewater/Stormwater Utilities (2004), issued by Water Environment Federation under the same EPA grant
www.wef.org/ConferencesTraining/TrainingProfessionalDevelopment/WaterSecurity/WEFSecurityGuidance.htm

Feature 5. Identify managers and employees who are responsible for security and establish security expectations for all staff.

- Explicit identification of security responsibilities is important for development of a security culture with accountability.
- At a minimum, utilities should identify a single, designated individual responsible for overall security, even if other security roles and responsibilities are dispersed throughout the organization.
- The number and depth of security-related roles will depend on a utility's specific circumstances.

Feature 5 Resource

Drinking Water Emergency Exercises - Summary Report
www.doh.wa.gov/ehp/dw/Publications/331-280_emergency_exercises_summary_report_1-12-05_web.pdf

B. Operational Features

In addition to having a strong culture and awareness of security within an organization, an active and effective security program makes security part of operational activities, from daily operations, such as monitoring of physical access controls, to scheduled annual reassessments. Utilities will often find that by implementing security into operations they can also reap cost benefits, and improve the quality or reliability of utility service.

Feature 3. Assess vulnerabilities and periodically review and update vulnerability assessments to reflect changes in potential threats and vulnerabilities.

Because circumstances change, utilities should maintain their understanding and assessment of vulnerabilities as a "living document," and continually adjust their security enhancement and maintenance priorities. Utilities should consider their individual circumstances and establish and implement a schedule for review of their vulnerabilities.

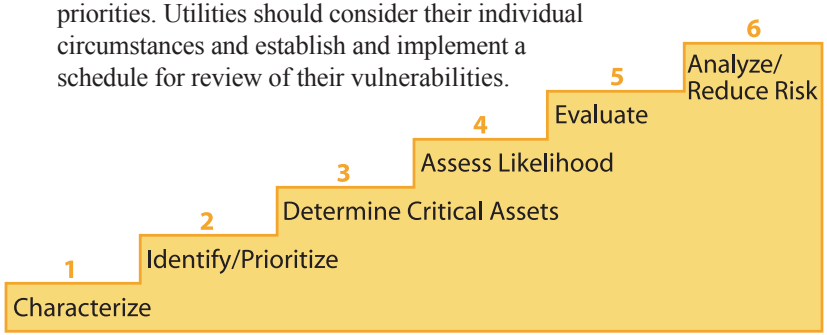


Figure 3. Steps for reviewing vulnerability assessments

Assessments should take place once every three to five years at a minimum. Utilities may be well served by doing assessments annually.

EPA has published guidance on the basic elements of sound vulnerability assessments; these elements are:

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

Feature 3 Resources

EPA Vulnerability Assessment Tools
cfpub.epa.gov/safewater/watersecurity/home.cfm?program_id=11
Security Information Collaboratives Guide
www.epa.gov/ordnhsrc/pubs/brochureSIC051805.pdf

Feature 4. Identify security priorities and, on an annual basis, identify the resources dedicated to security programs and planned security improvements, if any.

Dedicated resources are important to ensure a sustained focus on security. Investment in security should be reasonable considering utilities' specific circumstances. In some circumstances, investment may be as simple as increasing the amount of time and attention that executives and managers give to security. Where threat potential or potential consequences are greater, increased investment is likely warranted.

This feature establishes the expectation that utilities should, through their annual capital, operations and maintenance, and staff resources plans, identify and set aside resources consistent with their specific identified security needs. Security priorities should be clearly documented and should be reviewed with utility executives at least once per year as part of the budgeting process.

Feature 4 Resources

Grants and Funding
cfpub.epa.gov/safewater/watersecurity/financeassist.cfm
Small System Resources
cfpub.epa.gov/safewater/watersecurity/smallsystems.cfm

Feature 8. Define security-sensitive information; establish physical, electronic, and procedural controls to restrict access to security-sensitive information; detect unauthorized access; and ensure information and communications systems will function during emergency response and recovery.

Protecting IT systems involves using physical hardening and procedural steps to limit the number of individuals with authorized access and to prevent access by unauthorized individuals. Examples of physical steps to harden SCADA and IT networks include installing and maintaining fire walls, and screening the network for viruses. Examples of procedural steps include restricting remote access to data networks and safeguarding critical data through backups and storage in safe places. Utilities should strive for continuous operation of IT and telecommunications systems in the event of an emergency by providing uninterruptible power supply and back up systems, such as satellite phones.

In addition to protecting IT systems, security-sensitive information should be identified and restricted to the appropriate personnel. Security-sensitive information could be contained within:

- Facility maps and blueprints;
- Operations details;
- Hazardous material utilization;
- Tactical level security program details; and
- Any other information on utility operations or technical details that could aid in planning or execution of an attack.

Identification of security-sensitive information should consider all ways that utilities might use and make public information (e.g., during the competitive bidding processes for construction of new facilities or infrastructure). Finally, information critical to the continuity of day-to-day operations should be identified and backed up.

Feature 8 Resource

Protecting Water System Security Information
www.epa.gov/safewater/watersecurity/pubs/ncsl_foia_sept03.pdf

Feature 14. Develop utility-specific measures of security activities and achievements, and self assess against these measures to understand and document program progress.

Although security approaches and tactics will be different depending on utility-specific circumstances and operating conditions, the NDWAC recommends that all utilities monitor and measure common types of activities and achievements, including existence of program policies and procedures, training, testing, and implementing schedules and plans. These and other suggested measures are discussed in Section IV of this summary.

Feature 14 Resources

Security Vulnerability Self-Assessment Guide for Very Small Systems
http://asdwa.citysoft.com/_uploads/documents/live/5-31draftlatestv3.pdf
See also ***Booklet Section IV.A, "Utility-specific measures."***

C. Infrastructure Features

The NDWAC recommendations advise utilities to address security in all elements of utility infrastructure — from source water to distribution and through wastewater collection and treatment.

Feature 6. Establish physical and procedural controls to restrict access to utility infrastructure to only those conducting authorized, official business and to detect unauthorized physical intrusions.

Physical access controls include fencing critical areas, locking gates and doors, and installing barriers at site access points. Monitoring for physical intrusion can include maintaining well-lighted facility perimeters, installing motion detectors, and utilizing intrusion alarms. Neighborhood watches, regular employee rounds, and arrangements with local police and fire departments can support identifying unusual activity in the vicinity of facilities.

Procedural access controls include inventorying keys, changing access codes regularly, and requiring security passes to pass gates and access sensitive areas. In addition, utilities should establish the means to readily identify all employees including contractors and temporary workers with unescorted access to facilities.

Feature 6 Resources

EPA Security Product Guides
epa.gov/watersecurity/guide
Water Watchers Brochure
epa.gov/watersecurity/pubs/brochure_security_waterwatchers.pdf

Feature 7. Employ protocols for detection of contamination consistent with the recognized limitations in current contaminant detection, monitoring, and surveillance technology.

Until progress can be made in development of practical and affordable online contaminant monitoring and surveillance systems, most utilities must use other approaches. This includes monitoring data of physical and chemical contamination surrogates, pressure change abnormalities, free and total chlorine residual, temperature, dissolved oxygen, and conductivity.

Many utilities already measure the above parameters on a regular basis to control plant operations and confirm water quality. More closely monitoring these parameters may create operational benefits for utilities that extend far beyond security, such as reducing operating costs and chemical usage. Utilities also should thoughtfully monitor customer complaints and improve connections with local public health networks to detect public health anomalies. Customer complaints and public health anomalies are important ways to detect potential contamination problems and other water quality concerns.

Feature 7 Resources

The State of the Science in Monitoring Drinking Water Quality
www.epa.gov/ordnhsrc/pubs/reportEWS120105.pdf
WaterSentinel Pilot
www.epa.gov/ordnhsrc/pubs/fsWaterSentinel062005.pdf
Guidelines for Designing an Online Contaminant Monitoring System
www.asce.org/static/1/wise.cfm#MonitoringSystem

Feature 10. Monitor available threat-level information and escalate security procedures in response to relevant threats.

Monitoring threat information should be a regular part of a security program manager's job, and utility-, facility- and region-specific threat levels and information should be shared with those responsible for security. As part of security planning, utilities should develop systems to assess threat information and procedures that will be followed in the event of increased industry or facility threat levels. Utilities should be prepared to put these procedures in place immediately, so that adjustments are seamless. Involving local law enforcement and FBI is critical.

Utilities should investigate what networks and information sources might be available to them locally, and at the state and regional level. If a utility cannot gain access to some information networks, attempts should be made to align with those who can and will provide effective information to the utility on a timely basis.

Feature 10 Resources

Security Information Collaboratives Guide
www.epa.gov/ordnhsrc/pubs/brochureSIC051805.pdf
WaterISAC
www.waterisac.org
Water Security Channel
www.watersc.org
DHS Homeland Security Information Network (HSIN)
www.dhs.gov/dhspublic/display?theme=30&content=3813
CDC Health Alert Network
www.phppo.cdc.gov/han/

Feature 11. Incorporate security considerations into emergency response and recovery plans, test and review plans regularly, and update plans to reflect changes in potential threats, physical infrastructure, utility operations, critical interdependencies, and response protocols in partner organizations.

Utilities should maintain response and recovery plans as "living documents." In incorporating security considerations into their emergency response and recovery plans, utilities also should be aware of the National Incident Management System (NIMS) guidelines, established by DHS, and of regional and local incident management commands and systems, which tend to flow from the national guidelines. Adoption of NIMS is required to qualify for funds dispersed through EPA and DHS.

Utilities should consider their individual circumstances and implement a schedule for review of emergency response and recovery plans. Utility plans should be thoroughly coordinated with emergency response and recovery planning in the larger community. As part of this coordination, a mutual aid program should be established to arrange in advance for exchanging resources (personnel or physical assets) among utilities within a region, in the event of an emergency or disaster that disrupts operation. Typically, the exchange of resources is based on a written formal mutual aid agreement. For example, Florida's Water-Wastewater Agency Response Network (FlaWARN), deployed after Hurricane Katrina, allowed the new "utilities helping utilities" network to respond to urgent requests from Mississippi for help to bring facilities back on-line after the hurricane.

The emergency response and recovery plans should be reviewed and updated as needed annually. Utilities should test or exercise their emergency response and recovery plans regularly.

Feature 11 Resources

Emergency Response Tabletop Exercises for Drinking Water and Wastewater Systems CD
cfpub.epa.gov/safewater/watersecurity/trainingcd.cfm
Response Protocol Toolbox: Response Guidelines
www.epa.gov/safewater/watersecurity/pubs/rptb_response_guidelines.pdf
National Incident Management System (NIMS)
www.fema.gov/nims