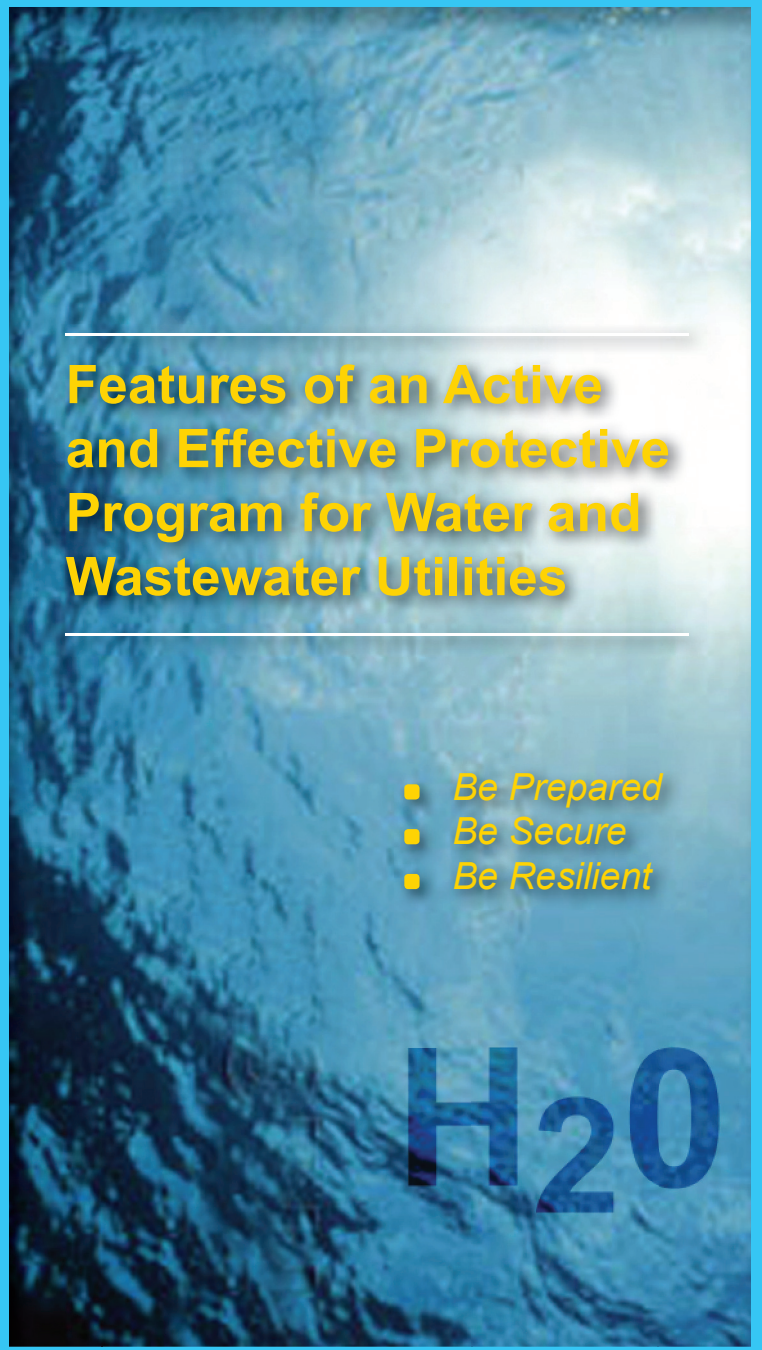
United States
Environmental Protection
Agency



United States
Environmental Protection
Agency

Office of Water (4601M)
EPA 817-F-08-005
www.epa.gov/watersecurity
October 2008

Office of Water (4601M)
EPA 817-F-08-005
www.epa.gov/watersecurity
October 2008

8. Does your utility receive screened, validated, and timely (e.g., in time to inform decisions or take action) threat information from one or more of the following sources (Y/N)?
   - WaterISAC
   - FBI
   - Local police
   - DHS

9. Do you have a plan in place to increase utility security in response to a threat (Y/N)?

10. Do you have a written business continuity plan (Y/N)?

11. Do you:
    - Have an emergency response plan (ERP) (Y/N)?
    - Conduct training on the ERP (Y/N)?
    - Carry out exercises on the ERP (Y/N)?
    - If so, which type:
      - Table top (Y/N)?
      - Functional (Y/N)?
      - Full field (Y/N)?
    - Review and update ERP on a periodic basis (Y/N)?

12. Has your utility adopted National Incident Management System (NIMS as part of its emergency response plan?
    - Is the Incident Command System (ICS) being used in your organization to manage incidents and/or preplanned events?

13. Is your utility a signatory to written agreements for requesting aid or assistance, such as an MOU for mutual aid and assistance or Water/Wastewater Agency Response Network (WARN) membership (Y/N)?
    - If no, are you in the process of creating an agreement (Y/N)?

14. Has your utility responded to an emergency request to provide mutual aid and assistance (Y/N)?

15. Do you have a crisis communication plan (Y/N)?

16. Do you engage in networking activities regarding emergency preparedness and collaborative response in the event of an incident (Y/N)?

More information on the measures and additional risk reduction measures for utilities, is available at: cfpub.epa.gov/safewater/watersecurity/measures.cfm.

- *WaterISAC, www.waterisac.org*
- *State and Local Fusion Centers, www.dhs.gov/xinfoshare/programs/gc_1156877184684.shtm*
- *CDC Health Alert Network, www.phppo.cdc.gov/han/*

Example Self-Assessment Measures

The Features establish the expectation that utilities should self-assess to measure progress and adjust their protective program based on performance data.

The water sector has developed measures of utility activities that roughly correspond with the activities described in the Features. *These measures are provided as examples for utilities to consider as a starting point as they develop their own self-assessment measures*.

1. Have you integrated security and preparedness into budgeting, training, and manpower responsibilities (Y/N)?

2. Have you incorporated security into planning and design protocols applying to all assets and facilities (Y/N)?

3. Do you routinely conduct supplemental monitoring or more in-depth analysis beyond what is required to identify abnormal water quality conditions (Y/N)?

4. Have you established relationships with public health networks to interpret public health anomalies for the purposes of identifying waterborne public health impacts (Y/N)?

5. Do you monitor and evaluate customer complaints for possible indications of water quality or other security threats (Y/N)?

6. Have you established protocols (i.e., consequence management plans) for interpreting and responding to indications of water quality anomalies (Y/N)?

7. Do you review your vulnerability assessment (VA) annually (Y/N)?
   - How frequently do you update your VA to adjust for changes in your system that may alter the risk profile of your utility? (never update; annually; every 2-3 years; every 3-5 years; every 5-10 years; no defined cycle)?

Features of an Active and Effective Protective Program for Water and Wastewater Utilities

Introduction

The water sector has developed the Features of an Active and Effective Protective Program to assist owners and operators of drinking water and wastewater utilities (water sector) in preventing, detecting, responding to, and recovering from adverse effects of all hazards, including terrorist attacks and natural disasters.

The Features originated as an outcome of a National Drinking Water Advisory Council workgroup in 2005 and have been updated to reflect the goals and objectives of the Sector Specific Plan for Water published in May 2007.

The Features use the terms "protective program," "protection," and "protective" to describe activities that enhance resiliency and promote continuity of service, regardless of the exact type of hazard or adverse effect a utility might experience.

The 10 features describe the basic elements of a "protective program" for owners/operators of utilities to consider as they develop utility-specific approaches. They address the physical, cyber, and human elements of prevention, detection, response, and recovery.

The 10 features:
- Are sufficiently flexible to apply to all utilities, regardless of size.
- Are consistent with the management philosophy of continuous improvement.

Water utilities can differ in many ways including:
- Source of water (ground or surface)
- Number of sources
- Treatment capacity

- Operational risk
- Locational risk
- Protective program budget
- Spending priorities
- Political and public support
- Legal barriers
- Public vs. private ownership

The goal in identifying common features of active and effective protective programs is to achieve consistency in protective program outcomes among water utilities, while allowing for, and encouraging, utilities to develop utility-specific protective program 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.

The Features

Feature 1. Encourage awareness and integration of a comprehensive protective posture into daily business operations to foster a protective culture throughout the organization and ensure continuity of utility services.

The objective of Feature 1 is to make protection a normal part of day-to-day operations.

Utility-specific efforts that help incorporate protection concepts into organizational culture might include:

- Senior leadership makes an explicit, easily communicated commitment to a program that incorporates the full spectrum of protection activities.
- Foster attentiveness to protection among front line workers and encourage them to bring potential issues and concerns to the attention of others; establish a process for employees to make suggestions for protection improvements.

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

Monitoring threat information should be a regular part of a protective program manager's job, and utility-, facility- and region-specific threat levels and information should be shared with those responsible for protective programs. As part of their planning efforts, utilities should develop systems to assess threat information and procedures that will be followed in the event of increased 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 (e.g. fusion centers). 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.

Utility-specific efforts might include:

- Develop standard operating procedures to identify and report incidents in a timely way and establish incident reporting expectations.
  - In the specific context of intentional threats and acts, ensure staff can distinguish between normal and unusual activity (both on/off site) and know how to notify management of suspicious activity.
- Develop systems to access threat information, identify threat levels, and determine the specific responses to take.
  - Investigate available information sources locally, and at the state or regional level (e.g., FBI Infraguard and Water ISAC).
  - Where barriers to accessing information exist, make attempts to align with those who can, and will, provide effective information to the utility.
- Make monitoring threat information a regular part of the protective program designee's job and share threat levels and information with key staff and those responsible for protection.

Feature 10 Resources

- *Guarding Against Terrorist and Security Threats: Suggested Measures for Drinking Water and Wastewater Utilities, USEPA 2004*

Feature 9. Develop and implement strategies for regular, ongoing communication about protective programs with employees, customers, and the general public to increase overall awareness and preparedness for response to an incident.

Effective communication considers 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 to consider are utility employees, response organizations, and customers.

Utility specific efforts might include:

- Establish public communications protocols, including prepared public announcement templates.
- Public communication strategies should:
  - Identify means to reach customers and the general public with incident information;
  - Provide a mechanism for customers and the public to communicate with appropriate personnel about unusual or suspicious events;
  - Inform customers about appropriate actions to enhance their preparedness for potential incidents that may impact services (e.g., reverse 911); and
- Internal communication strategies should:
  - Increase employee awareness of your protective program;
  - Motivate staff to support your protective program;
  - Provide ways for staff to notify appropriate personnel about unusual or suspicious activities;
  - Inform employees about the nature of, and restrictions on, access to security sensitive information and/or facilities; and
  - Ensure employee safety during an event or incident and enable effective employee participation during response and recovery efforts.
- Evaluate effectiveness of communication mechanisms over time.

Feature 9 Resources

- *Security Risk Communication Training, www.epa.gov/safewater/dwa/course-genint.html*
- *Effective Risk and Crisis Communication during Water Security Emergencies, www.epa.gov/ordnhsrc/pubs/600r07027.pdf*
- *Emergency Communications with your Local Government and Community | WERF Project 03-CTS-5SCO, www.werf.org*

- Identify employees responsible for implementation of protection priorities and establish expectations in job descriptions and annual performance reviews.
- Designate a single manager (even if it is not a full time duty) responsible for protective programs. Establish this responsibility at a level to ensure protection is given management attention and made a priority for line supervisors and staff.
- Keep current on improvements and good protective practices adopted by other utilities.
- Monitor incidents and available threat-level information; escalate procedures in response to relevant threats and incidents.

Feature 1 Resources

- *Seattle/King County Case Study, USEPA*
- *Chicagoland Case Study, USEPA*
- *Water Security Training Courses, Meetings, and Workshops/Webcasts, USEPA, cfpub.epa.gov/safewater/watersecurity/outreach.cfm*

Feature 2. Annually identify protective program priorities and resources needed, support priorities with utility-specific measures, and self-assess using these measures to understand and document program progress.

Dedicated resources are important to ensure a sustained focus on protective programs. Investment should be reasonable and consider 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 protective programs. Where threat potential or potential consequences are greater, increased financial 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 protective program needs. Priorities should be clearly documented and reviewed with utility executives at least once per year as part of the budgeting process.

This feature also encourages utilities to use metrics to self-assess and measure progress and to adjust their protective program based on performance data. Metrics should measure progress in physical upgrades, as well as personnel and process changes. Utilities are encouraged to develop utility-specific metrics relevant to their specific protective programs. As a starting

point, utilities can consider metrics that were developed at the national level, provided as examples in this brochure.

Utility specific efforts might include:

- Annually identify and dedicate resources to protective programs in capital, operations, and maintenance budgets; and/or staff resource plans.
- Tailor protective approaches and tactics to utility-specific circumstances and operating conditions; balance resource allocations and other organizational priorities.
- Annually review protection commitments and improvement priorities with top executives, rate setters, and water boards/commissions.
- Develop measures appropriate to utility-specific circumstances and operating conditions.
- Self-assess against performance measures to understand program progress and make necessary changes to improve effectiveness.

Feature 2 Resources

- *Grants and Funding, cfpub.epa.gov/safewater/watersecurity/financeassist.cfm*
- *National Metrics and Self Assessment Questions for Utilities, cfpub.epa.gov/safewater/watersecurity/measures.cfm*
- *VSAT™ Asset Management Module | WERF Project 03-CTS-6S, www.werf.org*

national public health, county health agencies, and health-care providers, such as hospitals.

Utility specific efforts might include:

- Forging partnerships in advance of an emergency, ensuring utilities and key partners are better prepared to work together if an emergency should occur.
- Join or help create a mutual aid and assistance network such as a Water and Wastewater Agency Response Network (WARN).
- Network with partners to stay aware of industry best practices and available protective program-related tools and training.
- Establish relationships with critical customers (hospitals, manufacturing, etc.) to identify interdependency issues that may impact business resiliency and continuity of business operations.
- Participate in joint exercises with identified partners as appropriate.

Feature 8 Resources

- *Security Information Collaboratives Guide, www.epa.gov/nhsrc/pubs/brochureSIC051805.pdf*
- *Waterand Wastewater Agency Response Networks (WARNs), www.nationalwarn.org*
- *Mutual Aid and Assistance Resources, USEPA, cfpub.epa.gov/safewater/watersecurity/maa.cfm*

Feature 7 Resources

- *Emergency Response Tabletop Exercises for Drinking Water and Wastewater Systems, cfpub.epa.gov/safewater/watersecurity/trainingcd.cfm*
- *Response Protocol Toolbox: Response Guidelines, www.epa.gov/safewater/watersecurity/pubs/rptb_response_guidelines.pdf*
- *EPA guidance documents on how to develop an ERP, cfpub.epa.gov/safewater/watersecurity/home.cfm?program_id=8*
- *National Incident Management System (NIMS), www.fema.gov/emergency/nims/*
- *2007 National Fire Protection Association (NFPA) 1600 standard on Standard on Management and Business Continuity Programs, www.nfpa.org/assets/files/PDF/NFPA1600.pdf*

Feature 8. Forge reliable and collaborative partnerships with first responders, managers of critical interdependent infrastructure, other utilities, and response organizations to maintain a resilient infrastructure.

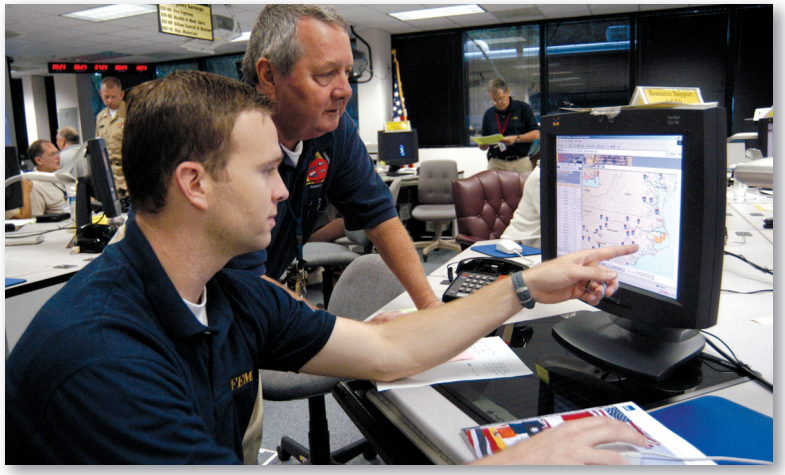
Effective partnerships build collaborative working relationships and clearly define roles and responsibilities so that people can work together seamlessly if an emergency should occur. It is important for utilities within a region, and within neighboring regions, to collaborate and establish a mutual aid program with one another and with neighboring response organizations, as well as, with interdependent sectors, such as the power sector, on which utilities rely or which they impact. Mutual aid agreements provide for help from other organizations that is prearranged and can be accessed quickly and efficiently in the event of an emergency.

Developing reliable and collaborative partnerships involves reaching out to managers and key staff in other organizations to build reciprocal understanding and to share information about the utility's 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 therefore, will be better able to serve each other.

Utilities and public health organizations should also establish formal agreements on coordination to ensure the 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—

Feature 3. Employ protocols for detection of contamination while recognizing limitations in current contaminant detection, monitoring, and public health surveillance methods.

Until progress can be made in development of practical and affordable online contaminant monitoring and surveillance systems, most utilities must use more traditional approaches, such as monitoring chlorine residual. Water quality monitoring, sampling and analysis, enhanced security monitoring, consumer complaint surveillance, and public health syndromic surveillance are different, but related, elements of an overall contamination warning system.



Water quality monitoring include 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 these parameters on a regular basis to control plant operations and confirm water quality. More closely monitoring these parameters may also create operational benefits for utilities that extend far beyond protective programs, 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 ("public health syndromic surveillance"). Customer complaints and public health anomalies are important ways to detect potential contamination problems and other water quality concerns.

Utility specific efforts might include:

- Establish sampling and testing protocols for events (and suspected events) and understand availability of, and be prepared to access, spe-

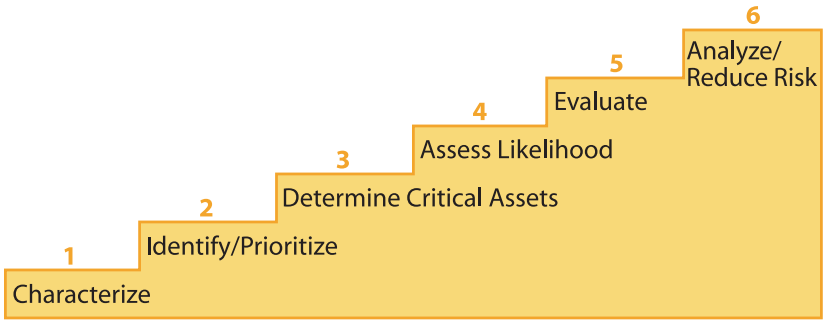
cialized laboratory capabilities that can handle both typical and atypical contaminants.
- Track, characterize, and consider customer complaints to identify potential contamination events.
- Use security monitoring methods (e.g., intrusion detection devices such as alarms or closed circuit television) to aid in determining whether a suspected contamination event is the result of an intentional act (Also see Feature 5).
- Establish working relationship with local, state, and public health communities to detect public health anomalies and evaluate them for contamination implications.

Feature 3 Resources

- *The State of the Science in Monitoring Drinking Water Quality, www.epa.gov/ordnhsrc/pubs/reportEWS120105.pdf*
- *Water Security Initiative, cfpub.epa.gov/safewater/watersecurity/initiative.cfm*
- *Guidelines for Designing an Online Contaminant Monitoring System, www.asce.org/wise*

Feature 4. Assess risks and periodically review (and update) vulnerability assessments to reflect changes in potential threats, vulnerabilities, and consequences.

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



Steps for reviewing vulnerability assessments

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

Utility specific efforts might include:
- Understand the NIMS guidelines established by DHS (as well as community and state response plans and FEMA Public Assistance procedures); and incident command systems (ICS). At a minimum, utility response and recovery planning should be NIMS compliant.
- Coordinate emergency plans with community emergency management partners:
  - Establish interoperable communications systems, where feasible, to maintain contact with police, fire, and other first responder entities.
  - Establish internal protocols to maintain communications with employees to ensure safety and to coordinate response activities.
- Implement backup plans and strategies for critical operations, including water supply and treatment (to mitigate potential public health, environmental, and economic consequences of events), power, and other key components.
- Know how to run your system manually (without SCADA).
- Maintain plans that are exercised at least annually, identify circumstances that prompt implementation, and identify individuals responsible for implementation.
  - Provide employees with appropriate preparedness and response training and education opportunities.
  - At least annually, review plans and conduct exercises that address a range of threats relevant to the utility.
  - Update plans, as necessary, to incorporate lessons from training, exercises, and incident responses.
- Ensure plans identify critical and time sensitive applications, vital records, processes, and functions that need to be maintained, and the personnel and procedures necessary to do so until utility has recovered. At a minimum, plans should include a business impact analysis and address need for power, communication (internal and external), logistics support, facilities, information technology, and finance and administration-related functions, including necessary redundancy and/or timely access to backup systems and cash reserves.

- Design and construction specifications should address both physical hardening of sensitive infrastructure and adoption of inherently lower risk technologies and approaches where feasible.
- Design choices should consider ability to rapidly recover and continue services following an incident.

Feature 6 Resources

- *EPA Security Product Guides, epa.gov/watersecurity/guide*
- *VSAT™ Asset Management Module | WERF Project 03-CTS-6S, www.werf.org*
- *Physical Security Guidance for Drinking Water and Wastewater Utilities, www.asce.org/wise*

Feature 7. Prepare emergency response, recovery, and business continuity plan(s); test and review plan(s) regularly update plan(s) as necessary to ensure NIMS compliance and to reflect changes in potential threats, vulnerabilities, consequences, physical infrastructure, utility operations, critical interdependencies, and response protocols in partner organizations.

Utilities should maintain response and recovery plans as "living documents." In incorporating protective program considerations into their emergency response and recovery plans, utilities also should be aware of the National Incident Management System (NIMS) guidelines, established by the Federal Emergency Management Agency (FEMA) within the Department of Homeland Security (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 protective program funds dispersed through EPA, FEMA 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.

Utility specific efforts might include:

- Maintain current understanding and assessment of threats, vulnerabilities, and consequences.
- Adjust continually to respond to changes in threats, vulnerabilities, and consequences.
- Establish and implement a schedule for review of threats, vulnerabilities, consequences, and their impact on the vulnerability assessment, at least every three to five years to account for factors such as facility expansion/upgrades and community growth.
- Reassess threats, vulnerabilities, and consequences after incidents and incorporate lessons into protective practices.
- Ensure individuals who are knowledgeable about utility operations conduct the reviews. Include an executive in the review process to provide an ongoing conduit of information to/from management.
- Use a methodology that best suits utility-specific circumstances and operating conditions; however, ensure the selected method supports the criteria outlined in the National Infrastructure Protection Plan (NIPP).

Feature 4 Resources

- *EPA Vulnerability Assessment Tools, cfpub.epa.gov/safewater/watersecurity/home.cfm?program_id=11*
- *VSAT™ Asset Management Module | WERF Project 03-CTS-6S, www.werf.org*

Feature 5. Establish physical and procedural controls to restrict access only to authorized individuals and to detect unauthorized physical and cyber 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 access gates and sensitive areas. In addition, utilities should establish the means to readily identify all employees, including contractors and temporary workers, with unescorted access to facilities.

Protecting cyber systems involves using physical hardening and procedural steps to limit the number of individuals with authorized access and prevent access by unauthorized individuals. Examples of physical steps to harden Supervisory Control and Data Aquisition (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.

Utility specific efforts might include:

- Identify and protect critical facilities, operations, components, and cyber systems (such as SCADA).
- Develop and implement physical and cyber intrusion detection and access control tactics that enable timely and effective detection and response.
- Utilize both physical and procedural means to restrict access to sensitive facilities, operations, and components including treatment facilities and supply/distribution/collection networks.
- Define, identify, and restrict access to security-sensitive information (both electronic and hard copy) on utility operations and technical details.
- Establish means to readily identify all employees (e.g., ID badges).
- Verify identity of all employees, contractors and temporary workers with access to facilities through background checks, as appropriate, per local/state law and/or labor contract and other agreements.
- Test physical and procedural access controls to ensure performance.

Feature 5 Resources

- *EPA Security Product Guides, epa.gov/watersecurity/guide*
- *Protecting Water System Security Information, www.epa.gov/safewater/watersecurity/pubs/ncsl_foia_sept03.pdf*
- *Physical Security Guidance for Drinking Water and Wastewater Utilities, www.asce.org/wise*
- *Control System Self Assessment Tool for Water Utilities | WERF Project 03-CTS-3SCO, www.werf.org*

Feature 6. Incorporate protective program considerations into procurement, repair, maintenance, and replacement of physical infrastructure decisions.

Prevention is a key aspect of enhancing protective programs. Consideration of protective 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 protective considerations into design choices, utilities need information about the types of protective design approaches and equipment that are available and the performance of these designs and equipment. For example, utilities should evaluate not just the way a particular design might contribute to protection, 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 protection and reduce vulnerability.

Utility specific efforts might include:

- Raise protective program considerations early in the design, planning, and budgeting processes to mitigate vulnerability and/or potential consequences and improve resiliency over time.