Implementing the Key Features

There are many ways of implementing the Key Features of an Active and Effective Protective Program. Following are examples of practices that water and wastewater utilities have implemented that help incorporate protection concepts into organizational culture. Utilities can select one or more of these activities to implement in their own protective program to improve its effectiveness.

For additional examples, the Key Features case studies provide summaries of how utilities are implementing the Key Features.

1. Integrate protective concepts into organizational culture, leadership, and operations

- 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.
- 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) to be responsible for protective programs. Establish this responsibility at an appropriate 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.

2. Identify and support protective program priorities, resources, and utility-specific measures

- 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.

3. Employ protocols for detection of contamination

- Establish sampling and testing protocols for events (and suspected events). Understand availability of, and be prepared to access, specialized 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 relationships with local, state, and public health communities to detect public health anomalies and evaluate them for contamination implications.

4. Assess risks and review vulnerability assessments

- 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 (at least every three to five years) to review threats, vulnerabilities, and consequences, and their impact on the vulnerability assessment, in order 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).

5. Establish facility and information access control

- Identify and protect critical facilities, operations, components, and cyber systems (such as Supervisory Control and Data Acquisition (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 the identity of all employees, contractors and temporary workers with access to facilities. Use background checks, as appropriate, per local/state law and/or labor contract and other agreements.
- Test physical and procedural access controls to ensure performance.

6. Incorporate resiliency concepts into physical infrastructure

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

7. Prepare, test and update emergency response, recovery and business continuity plans

- Understand the National Incident Management System (NIMS) guidelines established by Department of Homeland Security (DHS) (as well as community and state response plans and Federal Emergency Management Agency (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 responders.
    - 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, power, and other key components, to mitigate potential public health, environmental, and economic consequences of events.
- Know how to run the 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.

8. Develop partnerships with first responders, managers of critical infrastructure, other utilities and response organizations

- Forge partnerships in advance of an emergency, ensuring utilities and key partners (e.g., emergency responders) 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.

9. Develop and implement internal and external communication strategies

- 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; and
    - Inform customers about appropriate actions to enhance their preparedness for potential incidents that may impact services (e.g., reverse 911).
- 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.

10. Monitor incidents and threat-level information

- 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.