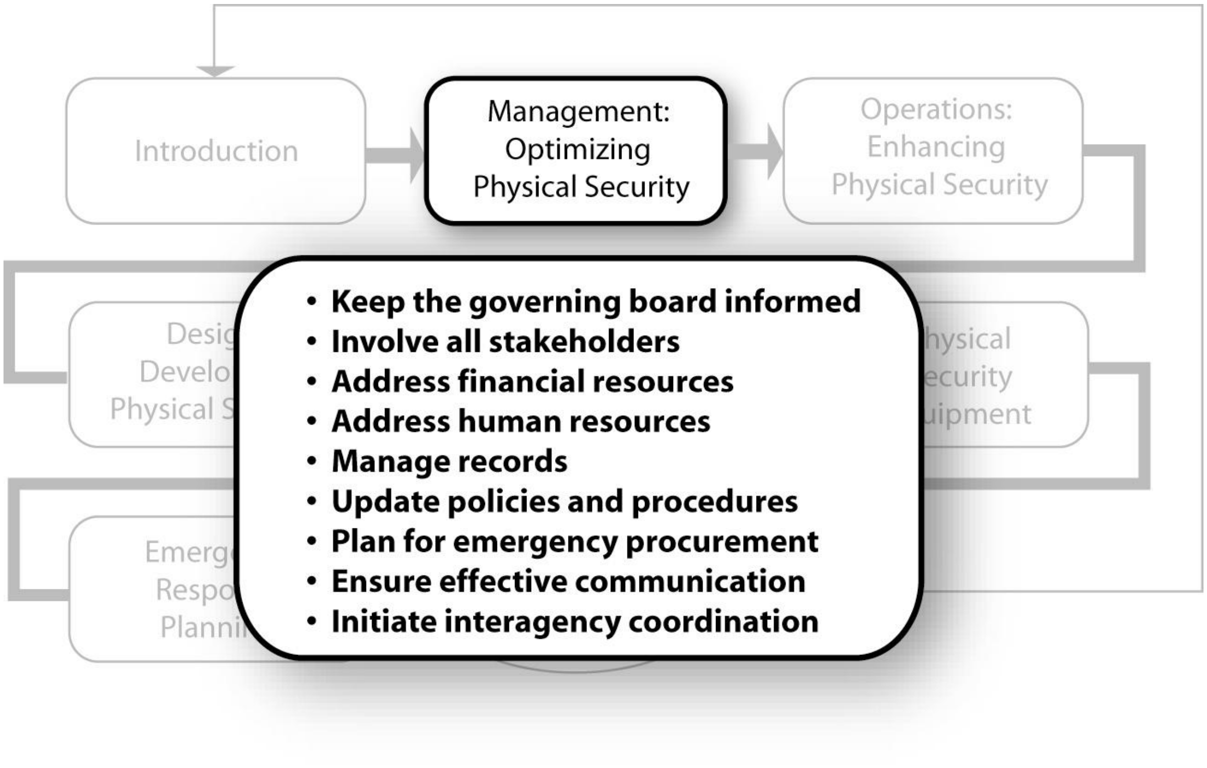
SECTION 2

Management Considerations for Optimizing Physical Security


Introduction
Management: Optimizing Physical Security
Operations: Enhancing Physical Security
Desig
Develo
Physical S
hysical
ecurity
uipment
Emerg
Respo
Planni
• Keep the governing board informed
• Involve all stakeholders
• Address financial resources
• Address human resources
• Manage records
• Update policies and procedures
• Plan for emergency procurement
• Ensure effective communication
• Initiate interagency coordination

2.1 Overview

Many measures available to water utilities to reduce the risks associated with malevolent actions and, to a great extent, natural disasters are those that can be developed and put into effect without concrete, metal, or heavy equipment. While all utilities should make the development of security-enhancing policies and procedures a priority, it is especially important that smaller utilities and those with limited resources make the most from these low-cost/high-value actions, rather than being frustrated by the inability to fund major infrastructure countermeasures. These actions include organizational cultural changes, employee training, stakeholder awareness, and policies and procedures that change business practices with the goal of a more secure workplace and better protected facilities.

Utility management can implement these security enhancements for a relatively low cost and in a manner designed to augment physical security measures that may be added at a later date. This section provides concepts, strategies, and actions that water utility managers can consider when contemplating how to possibly prevent and better prepare for both known and unknown challenges that may arise.

As with all sections in this guidance, this section is not designed to be prescriptive, but rather as an aid based on best practices used by the most efficient, effective, and secure water utilities in the United States. It is also designed to guide management as it applies security considerations, even though physical security upgrades may not yet be in place.

A reminder, as mentioned earlier in this document, that physical security is related to, but not the same as, protection from natural disasters. Planning for natural disasters has been part of management's responsibilities for decades. Protecting utilities against malevolent acts has become a higher priority due to recent events. Preparedness, mitigation, response, and recovery for the threats and hazards of human-caused events are more complex, requiring continuous re-evaluation of the motivation and mindset of the threat.

2.2 Governing Board

The governing board of a water utility, whether comprising elected or appointed persons, is the policy-making body of the utility. The board is ultimately responsible to the utility's customers for ensuring proper management of the water system to maintain public health and to protect the environment. From this standpoint alone, it is important for utility management to provide governing board members with, at a minimum, a high-level overview of water system threats and vulnerabilities and management's approach to mitigating the associated risks. However, because it is likely that governing board approval will be required to implement policy changes and physical security improvements that may impact capital and operations budgets, utility managers should consider providing board members with more detailed information about water system security.

Possibly, the biggest obstacle to implementing security measures will be convincing the governing board that water systems are indeed vulnerable. Utility managers may find it helpful to reference the nationwide emphasis on securing water infrastructure.

- Consider describing EPA's Strategic Plan for Homeland Security and the development of tools and guides by AWWA, the American Water Works Association Research Foundation (AwwaRF), and AMWA to assist in the assessment of water system vulnerabilities and in the reduction of security-related risks.
- Use factual occurrences as examples—illegal entry in distribution system storage reservoirs, intentional and accidental dumping into a river or lake upstream of a water treatment plant, loss of equipment due to criminal activity, or vandalism at a remote pump station that could have resulted in water outages or financial impacts to the utility—to emphasize the importance of water system security.
- Discuss how a security breach can impact public health, place utility employees at risk, and damage the environment.
- Examine the effect of an incident for which the utility was unprepared on the credibility of the utility and the governing board.

- Focus on opportunity cost versus the cost of not implementing security measures, including possible liability and regulatory action, should the utility not address obvious vulnerabilities or take reasonable security measures.
- Provide the governing board more than just the consequences; provide management's approach to responding to the challenges by realistically forecasting short- and long-term needs and the impact on resources, such as labor costs, other operation and maintenance (O&M) costs, and capital, as well as on developing funding alternatives.
- Preparing and protecting against man-made events also serves the dual purpose of protecting facilities against the effects of natural disasters.

While communication with the governing board is imperative, utility managers must be cautious about those security details that might be revealed in public forums. Therefore, discussions about water security with governing board members should be held privately if state and local sunshine laws allow. Sunshine laws and the Freedom of Information Act (FOIA) stipulate the types of discussions that can take place with board members outside of public meetings and how many board members can meet without public notification. Sunshine laws are laws aimed at opening up government procedures to inspection by the public, metaphorically letting the "sun shine" on the procedures (http://WordIQ.com/definition). For example, the Ralph M. Brown Act governs open meetings in California for local government bodies, such as boards, councils, and commissions. This law guarantees the public's right to attend and participate in meetings of local legislative bodies. Because laws vary from state to state, utility managers should seek guidance from their legal counsel so that their efforts to keep discussions about security measures confidential do not violate the law. In general, at public meetings, utility managers should refrain from long and detailed descriptions of security needs and measures. If board members are briefed in closed sessions not open to public participation, detailed public discussions should not be necessary.

Utility agencies should also consider formalizing these procedures, briefings, approval levels, and responsibilities in a written security policy. A security policy can clarify what can and what cannot be discussed in open forum, as well as outline the level of expectations of the city staff, the management staff, and the utility staff in securing water facilities.

2.3 Customers and Other External Stakeholders

Utility managers may want to be prepared to respond to questions from customers, the media, and other external stakeholders who may want to know if or why water security is an issue and what the utility is doing to reduce risks to infrastructure, persons, and service. These external stakeholders may include community organizations and environmental activists who are interested in the countermeasures that the utility may use to prevent or mitigate the effects of events such as a chemical or biological contamination, disruption of drinking water supply, and loss of fire flow. Other external stakeholders may be government agencies, elected officials, and business owners who want assurance that the utility has taken the appropriate steps to maintain service during malevolent or natural disasters.

Unlike other utility matters, proactive communications with all customers and external stakeholders about security measures may not be necessary or even desired due to the confidential nature of the subject. However, utilities can initiate discussions about water security with a few categories of external stakeholders (such as law enforcement, and fire and health departments) to improve the planning and implementation of countermeasures and emergency response.

Water utility managers should also initiate discussions with wholesale customers—those cities, counties, or companies operating regional water systems that provide water to a number of downstream retail water providers. Wholesale customers can be encouraged to protect their water systems at the same level of protection as that used by the wholesaler's retail customers. New or renewed wholesale agreements can include requirements for the wholesaler to institute countermeasures to mitigate risk to the utility's water system.

Implementation of security measures could have substantial impacts on water system budgets, both capital and operating. Whether the utility will fund security projects from debt sources or net revenue, pressure on water rates may necessitate a rate increase. Thus, utility managers will need to inform customers of the importance of security measures in providing uninterrupted service and protection of public health and the environment, without revealing significant details about the approach to security or specific countermeasures. Water utilities may want to consider a specific surcharge on the base water rate to fund security projects. An example of this strategy is shown in Figure 2-1. (CleanWaterAtlanta 2004).

> **City of Atlanta – Ordinance 03-O-2212**
>
> SECTION 7: (a) That the imposition of a surcharge shall be placed on all domestic, commercial, industrial and other users of the City of Atlanta Water and Wastewater System to pay for the cost to implement the security and infrastructure requirements as described in the Safe Drinking Water Act and Public Heath Security and Bioterrorism Preparedness and Response Act. (b) that for purpose of this ordinance, the surcharge will be described as the "Water and Wastewater Systems Security Surcharge." (c) that the Water and Wastewater Systems Security Surcharge shall be $0.15 per hundred cubic feet for all billing cycles beginning on and after January 1, 2004. Funds collected from the surcharge shall be deposited in a fund separate and distinct from other funds of the Water and Wastewater System.
>
> Enacted January 2004

FIGURE 2-1
Sample Surcharge Language

Proactive communication with other water utilities, regulatory agencies, and first-responders is also important to developing and maintaining a secure system, as described in Section 2.9, "Communications."

2.4 Financial Planning

When looking for opportunities to facilitate ways improve security, financial planning presents a very important opportunity to reduce risks. Key areas include:

- Developing Capital Improvement Plan (CIP) programs that adequately support security needs.
- Integrating Government Accounting Standards Board Statement 34 (GASB 34) considerations with the CIP planning for security and reporting purposes. The following is the time line for actions in the near future (see www.GASB.org for latest requirement details):

  - Phase 1 public entities – those with total annual revenues equal to or greater than $100 million; actions are required for fiscal years beginning after June 15, 2005.
  - Phase 2 public entities – with total annual revenues equal to or greater than $10 million but less than $100 million; actions are required for fiscal years beginning after June 15, 2006.
  - With the exception of, "Public Institutions that report as special-purpose Governments engaged only in business-type activities are required to report infrastructure upon implementation, without regard to the phase-in periods included in this paragraph. The transition period also does not apply to business-type activities for public institutions engaged in both governmental and business-type activities."
- Developing a diversified strategy for funding both capital and operating needs that can be supported by governing boards and customers.

Of these considerations the first three are described in more detail below.

2.4.1 Developing CIP Programs that Adequately Support Security Needs

To meet normal customer demands on the systems and to accomplish security objectives, water utilities invest in CIP programs and O&M programs to keep existing facilities at proper functioning levels. Utilities may also need to modify or build additional facilities that have been identified as key to improving security. Building facilities with improved security take a variety of forms, such as providing redundancy where it currently may not exist, improving flexibility and management of existing facilities, and restricting access to critical facilities.

It is obvious that having an adequate and integrated CIP and funding program is essential because security-related projects often need to compete with many other capital projects, such as:

- **System Growth Requirements.** Many water systems with growing and developing population bases need to spend substantial funding on capital projects to develop new raw water supplies, expand treatment capacity, or extend distribution system networks to new areas.
- **Correction of Identified Deficiencies Not Related to Security.** Many utilities have neglected aging assets. Inventory work and condition assessments conducted as part of asset management programs have, in many cases, quantified the need for action to make up for past neglect.
- **"Normal" Renewal and Replacement.** Well-managed water utilities proactively plan to spend a steady amount on the orderly renewal and replacement of aging system components. While these projects contribute to the overall integrity of the systems in the long run, in the short run the funding for these projects may compete with specific security-related investments that have high priority.

These competing considerations make it increasingly important for water utilities to have sound processes for identifying, prioritizing, and implementing their capital improvement programs. Traditionally, water utilities have identified required projects but have not prioritized the projects or documented how the projects relate to key goals and objectives of the utilities. Increasingly, utilities are turning to more systematic decision management methodologies that identify and weigh criteria, and then explicitly “score“ the performance of candidate projects. In such systems, security considerations could be explicitly recognized as a criterion and weighed in relation to other competing priorities.

The Capital Planning Strategy Manual, published by AwwaRF and AWWA in 2001, includes instructions and tools for implementing these more systematic prioritization decision management methodologies. These approaches are sometimes called multi-attribute utility models because scales are created that measure the contribution (value) added using both monetary and non-monetary criteria. In addition, cost-benefit relationships can be identified to guide the planning process. The decision management process can then include the efficiency of candidate projects toward meeting fundamental agency objectives such as security. By selecting the projects that most efficiently contribute to stakeholder goals, it is possible to identify a 5-year, 10-year, or 20-year series of capital expenditures that maximizes the value of security and other goals within identified annual levels of capital expenditure.

For smaller utilities without a large CIP or operating budget, the increased attention on simple, effective O&M procedures becomes more important in protecting crucial functions of the system from threats.

To satisfy both normal renewal and replacement needs as well as security needs, normal activities can include appropriate security improvements. For example, when a tank is taken out of service for repair/repaint, use the opportunity to modify valves, vents, hatches, ladders, etc. to enhance the security of the tank.

Implementing security considerations on existing and new facilities, and the construction of new facilities to meet growing customer demands, are not mutually exclusive activities. Rather, they are similar in planning the dollar investment requirements. Normal or routine maintenance and renewal of assets can be coupled, where it makes sense, to changes in how systems operate or to include physical security improvements. New system facilities can be designed with those changes already in place as part of construction and operational functions that help promote security consciousness.

2.4.2 Developing Funding Programs to Support Operating Fund Needs

Developing funding programs that support the operating funds of a water utility is also critical to reducing risks related to security. Defining and securing stakeholder and governing board support for operating budgets supports risk reduction in a number of ways. The labor budget (or contract budget where operations are performed through a private vendor) literally provides the funding support for the crews that maintain, operate, and monitor the water utility’s assets. Inadequate labor budgets present several labor-related risks, including:

- Possibility of facility breakdowns (e.g., loss of the WTP or a break in a major distribution system segment) that escalate into emergency situations because the situations go undetected during the period in which there is still an opportunity for recoverable intervention.

- Risk that power failures, software system failures, computer viruses, or other system failures will go undetected if there is inadequate or insufficiently trained staff to monitor and react to these types of security threats.

In addition to providing the labor required to adequately staff the system, the operating budget contributes to risk reduction/security enhancement by providing funding for operations and maintenance of security systems, as well as general equipment and supplies needed to keep the system in proper working order.

Beyond these basic labor and equipment/supply considerations, the operating budget contributes to risk reduction/security by providing funding needed for the services listed below:

- **Operating Reserves.** Numerous utilities have set an internal goal of maintaining a minimum of one billing cycle's worth of operating budget to be set aside in reserve so that utilities can make payments required in the event of a crisis. Depending on the utility, as much as 90 to 120 days' worth of operating budget may be required.
- **Petty Cash/Liquid Funds.** Cash on hand is needed to support immediate needs such as funding emergency activities or allowing transactions with customers or vendors that do not have access to alternate payment tools.
- **Debt Service Coverage.** Many water utilities fund at least a portion of their capital programs through municipal bonds or through state revolving fund loans. In most cases, these funding vehicles require that net revenues for the utility be adequate to provide some level of coverage above the annual debt service payments. The required level varies but is often in the range of 1.10 to 1.25 times the annual debt payment. For utilities with substantial outstanding debt, the coverage amount can represent millions of dollars. Water utilities that do not provide adequate operating budgets to satisfy the coverage provisions for their bonds run the risk that their credit ratings will decline and that they will not be able to incur additional debt for security-related capital projects. In addition, bond covenants often require that utilities maintain specified levels of funding such as debt service funds, debt service reserve funds, and emergency funds.

A sometimes overlooked element of operating fund adequacy relates to customer billing and collection systems and processes. It is critical to long-term financial stability that utilities maintain high collection rates for their bills or customers will stop paying the bills. Maintaining up-to-date customer and collection records and taking prompt action to collect on unpaid bills are essential to credibility. Therefore, it is important for utilities to consider the security and resilience of billing and collection systems in their vulnerability assessments.

2.4.3 Developing a Funding Program that Governing Boards and Customers Can Support

In addition to developing budgets that reasonably support the capital and operating funds that are needed to improve security, water utilities need to develop budgets and funding programs that their decision-making boards and customers will support. To gain support from governing boards, utility staffs increasingly need to be able to document that:

- Proposed capital programs are justified (i.e., supported by a prioritization process, such as a vulnerability assessment, and integrated with other capital needs through an asset management program such as the one described in Section 2.4.1, "Developing CIP Programs That Adequately Support Security Needs").
- Proposed rate and fee structures are equitable and supportable.
- Proposed financing plans for capital programs are optimal. For example, boards increasingly want an evaluation (e.g., degree of bonding vs. equity funding, level debt structure vs. balloon payments) of several financial planning scenarios to determine whether the selected path is consistent with the utility's goals and objectives.
- Adequate outreach to all segments of the customer base regarding proposed rate increases or changes in the rate and fee structures has been performed.

Boards understand the value proposition in the utility's overall planning process. Instead of just performing a standard rate or revenue requirements study, utility systems are increasingly deciding to conduct strategic or business planning studies that consider the merits of expanding or contracting the activities that are conducted by the utility.

Customers and other stakeholders are increasingly sophisticated in their attention and interest in water rate and financial considerations. To obtain support for rates and charges that support the capital and operating funds required to reduce risks, utilities need to demonstrate to their customers that:

- Proposed rates and charges are fairly divided among the system's customers and customer classes.
- Rates and charges are affordable in light of income within the community and in comparison with rates and charges in neighboring communities.
- Proposed spending by the utility is justified.

For additional information on water rates, see the 2004 AWWA Water Utility Council-sponsored study titled, "Avoiding Rate Shock: Making the Case for Water Rates."

2.5 Human Resources

Just as employees are critical to the successful operation of a water system, they are also critical to ensuring a secure water utility. Employees are "insiders"; they have unique knowledge of the water system's infrastructure, processes, and vulnerabilities. They are authorized to access both facilities and information; if that access is used with malicious intent, the results could be catastrophic. Consequently, water utility managers are taking measures to mitigate the risks posed by new, existing, and former employees.

Numerous federal, state, and local laws pertain to employee rights and the employer-employee relationship. These laws determine the security measures that water utility managers can and cannot take when employees are involved. In addition, bargaining unit agreements will undoubtedly address employer-employee relations and may restrict the employer's use of otherwise lawful security measures. It is imperative that a utility's legal counsel be consulted before any security measures involving employees are implemented, including those discussed in this document.

Employees can provide a vital role in ensuring that the water system is kept secure thorough heightened awareness and adherence to policies and procedures. To gain employee buy-in, consider beginning with security awareness training for all employees as part of new employee orientation. This training can provide an overview of the vulnerabilities faced by water utilities and the threats that must be protected against. Employees can receive an explanation of new and proposed security policies and be instructed on how they can assist in reducing security risks.

To integrate security concepts into the organizational culture, utility management can emphasize security in its actions and communications. Some suggestions include:

- Discuss security with the staff during formal and informal meetings.
- Make security an agenda item at every staff meeting.
- Provide employees with adequate security training (see Section 2.5.6, "Training").
- Develop security policies and procedures and enforce them consistently and equitably.
- Include initial and recurring background investigations and quarterly employee reviews in addition to annual performance reviews.
- Consider creating a position of utility security officer, or expand the responsibilities and authority of an existing position (e.g., the safety officer).
- Give the individual(s) assigned responsibility for security the appropriate authority to correct shortcomings and take necessary actions.
- Include articles on security in internal newsletters.

The approach to integrating security into the culture of the utility is similar to the process used to integrate worker safety into all aspects of utility operations. While employees do not become security guards (security guards are outside hires best suited for a temporary situation), full-time, permanent employees offer the knowledge and awareness capability to detect, discern, and deny an outsider from causing an emergency situation within the utility.

2.5.1 Background Checks

Utilities may want to consider adopting a practice of conducting basic background checks of applicants for utility positions. Typically, such background checks can include confirming past employment, education, professional certifications, and references, as well as any facts available through public records. Advertisements and notices for positions should include a statement that background checks are required, and applications for employment should include a waiver whereby the applicant allows the background check and also authorizes the applicant's former employers to speak with the utility. Background checks should be completed before job offers are made, or job offers should be contingent on a background check. If lawful and if consistent with bargaining unit agreements, background checks with periodic reviews should also be conducted for current employees.

Consideration should also be given to expanding the background check to include criminal and other records such as driver's license, worker's compensation, military service, credit history, and possibly character references. Be aware, however, that there may be significant legal restrictions and liability associated with enhanced background checks. Whatever level of background check is conducted, it is imperative that the utility maintains consistency for all applicants or for all who apply for a specific position.

It should be noted that background checks are sometimes faulty and need to be confirmed through other channels, if possible. For example, criminal background checks may be incomplete or erroneous. Local law enforcement agencies may only have criminal records of those persons living or convicted within their jurisdiction. On the other hand, national databases may not contain information from cities and counties unless such data was input specifically into the national system. Similarly, credit records may be incomplete or inaccurate.

A more thorough discussion on the subject of background checks is contained in the AMSA publication entitled, "Legal Issues in a Time of Crisis Checklist."[3]

2.5.2 Identification Badges

Depending on the size of the utility operation, the use of employee identification (ID) badges may be considered. If so, the following paragraphs provide important areas to consider. If employee badges are not used, employees still need to understand and act on the presence of unauthorized individuals on utility jurisdictions areas.

Employee ID badges provide instant verification of whether individuals are authorized to be at a utility's facility or to handle utility equipment. Color-coded badges can be used to alert others if employees are in an inappropriate area and can deter employees from straying into restricted areas. ID badges can contain an up-to-date color photo of the employee, along with a date of expiration. Both the photo and date of expiration, and color code if used, should be visible from a distance of several feet. Renewal of ID badges may occur at a period not to exceed 2 years from the date of issue. The badges may contain security features such as holograms, watermarks, as well as magnetic strips or radio frequency identification (RFID) devices that permit access to designated areas and track locations of employees.

All employees, including temporary and part-time employees, interns, and volunteers, should be issued ID badges and be required to wear them in plain sight. Employees who forget their badges or who are visiting other utility locations should be issued temporary ID badges. Such badges should, at a minimum, be time-sensitive or light-sensitive so that the "age" of the badge is visibly apparent. In addition, or as an alternative, authorized personnel may escort employees visiting locations outside of their authorized areas.

[3] Association of Metropolitan Sewerage Agencies. 2002. *Protecting Wastewater Infrastructure Assets…Legal Issues in a Time of Crisis Checklist.*

Removal and storage of employee badges when outside of the work areas should be a regular practice, as well as when in public areas away from work. In terms of security, security badges should not be visible to others who may want to copy the design.

2.5.3 Employee Surveillance

Employee surveillance serves two purposes: to enhance employee safety and to monitor potential insider threats. While surveilling employees may seem to indicate that utilities' do not trust their employees, this topic is included because the focus of this guidance is the increased security of utilities and their assets.

Monitoring of employee activities at their workplace may be subject to federal and state privacy laws. In general, however, it is acceptable to routinely monitor employee use of electronic media, such as e-mail and Internet surfing. Depending on the size of the utility operation, the use of closed-circuit television (CCTV) or other forms of video monitoring may be implemented. Monitoring of employees through CCTV cameras is also typically acceptable, as long as the cameras are visible to employees. One important prerequisite of employee surveillance is notifying employees that they are being monitored; otherwise, the employees may have a reasonable expectation of privacy in their work area, and the utility may face legal challenges to information obtained in this way.

Some utilities have taken a simpler approach and implemented a buddy system for entry into critical facilities. However, to make this system effective, some type of recognition hardware needs to be in place, such as cameras or access card readers.

2.5.4 Employee Response

Effective reaction to, and recovery from, malevolent or natural events depends upon a rapid and thorough response by a knowledgeable and experienced workforce. Utility management should develop policies and contingency plans to address problems that employees may have traveling to utility sites and facilities during and after an incident. Additionally, management should be aware that employees may decide to remain at home with their families or evacuate from the vicinity if a disaster should occur, thereby leaving the utility without needed labor and expertise. Utility management may want to consider developing a family shelter/evacuation plan that will provide employees a level of confidence that their families are safe while they respond to their duties at the utility. Human resource policies should address what will be considered an acceptable excuse for not responding to work during an incident, or even if a severe malevolent act advisory is declared, and what action should be taken for non-excused absences. It is important to note that such policies should be determined with a thorough understanding of the utility's legal responsibilities governing employee leave, including relief allowed employees under the Americans with Disabilities Act.

While many of these issues can be addressed in company human resources policies and procedures, they can be repeated in the ERP, as discussed in Section 7, "Emergency Response Planning."

2.5.5 Contractors

It is important that utility managers consider not only their own employees as a potential insider threat, but also contractors who may have access to utility facilities and information at any given time. Venders, delivery personnel, service providers and outside utility representatives can also be considered potential insider threats.

Suggested contractor security procedures include:

- Establishing good sign-in and sign-out procedures (e.g., requiring a photo ID that matches the individual and his or her signature) and limiting access to sensitive areas (such as chemical areas and SCADA controls).
- Requiring visitors to sign in and wear a visitor badge so contractor employees are easily identified. All visitors and badges should be accounted for at the end of the day.
- Requiring escorts if physical barriers are not present.
- Limiting use of private vehicles at the utility's sites.
- Remote read meters could be installed to limit some outside access, and deliveries can often be made to other locations not located near sensitive or critical operational areas.
- Evaluating the environmental, health, and safety record of contractors before signing contracts; considering offering environmental health and safety training to contractors onsite.
- Performing background checks on contractor personnel assigned to project sites. While this is a sometimes difficult activity, it could be considered depending on the situation.

In addition, for construction contractors the following could be considered:

- Locking construction gates at end of the day and when not in use; using interlocking padlocks with utility locks.
- Evaluating potential misuse of heavy equipment and taking appropriate measures.
- Considering ways of securing heavy equipment each night.
- Considering additional fencing and separate entrance, separate parking areas, and guards to coordinate construction staff.

2.5.6 Training

To ensure that a security program is effective, the staff can be trained in many aspects of security and emergency response. With improved security actions comes a new culture for water professionals. This section discusses types of training and training resources important for utility staff.

2.5.6.1 Types of Training Sessions

Utilities can make their own determinations regarding the variety and level of detail relevant to their situations. Initial and recurring training sessions can also be scheduled to reduce impacts to operational budgets.

Table 2-1 lists training relevant categories that may be applicable to a complete spectrum of water utility personnel. If a particular training is more important for one group of personnel, that group is listed in the Notes column.

The main training type categories, as listed vertically in the first column, are subjects to which all utility employees should be introduced. The specific areas, and the length and breadth of the training may vary depending on size and scope of utility operations, and should be tailored to each situation.

Depending on budgets and schedules, a timetable should be established to have everyone reach basic comprehension of the categories listed. Once achieved, further training, certifications or proficiency levels, joint exercises, and the like can be planned on a more periodic basis.

2.5.6.2 Location of Training Exercises

Many state and local resources are available to conduct, and sometimes fund, training for utility staff. When considering training, it is a good idea to check with city and county administration, police departments, fire departments, local emergency planning agencies, local health departments, and the Red Cross to inquire about available training. Nearby utilities may want to participate in training sessions and contribute funding.

2.5.6.3 Staff Motivation

Staff often complain about attending training sessions, especially when their daily jobs are busy. There are several incentives to help motivate staff to attend training:

- Provide certification toward professional development hours
- Require training as part of employee evaluations
- Further career goals/personal development

Providing lunch or snacks during a training session can also help to make the day more efficient and enjoyable.

2.5.6.4 Cross-training

Training staff members in skills outside of their normal duties may be prudent so that multiple staff members can perform needed tasks in times of emergency. For example, operators should understand basic maintenance of pumps, motors, and electrical components. Likewise, maintenance workers should understand the basics of treatment plant operations. A cross-training program should involve treatment plant workers spending time with and learning the skills of distribution system workers, as well as gaining knowledge of the raw water input system. A cross-training program also provides a more flexible workforce that will not only improve response during an emergency situation, but will also allow for improved efficiencies during normal operations. Planning for a cross-training program may need to involve the utility's bargaining unit and human resource professionals.

TABLE 2-1
Types of Security and Emergency Response Training Relevant for Water Utility Personnel

Training Type	Purpose	Benefit	Description	Resources to Provide Training	Notes
Security Awareness and Understanding Standard Operating Procedures	To provide staff with security awareness basics and familiarize staff with general utility security procedures.	Facilitates a security-conscious culture at the utility. Brings standard operating procedures to the foreground.	Provides the means to identify potential security concerns on a daily basis. This may include information on physical and cyber security, as well as suspicious persons. The course also reviews basic security procedures in use by the utility.	Police Department; Internal Staff; Consultant	
How to Handle Disgruntled People	To assist the public in a calm and effective manner; to more effectively manage employees.	Minimizes complaints, improves customer satisfaction, maintains positive customer relations, minimizes internal employee threats; encourages consistent threat documentation procedures.	Provides background in understanding human behaviors; teaches various methods to handle upset customers; practices techniques in various situations.	Police Department; Consultant; Human Resources Personnel	Especially important for managers and employees interacting with the public
Understanding the Emergency Response Plan	To familiarize staff with the plan.	Enhances efficiency in emergency response.	Includes a walk-through of sections; reviews location of information.	Safety Coordinator; Consultant	Employees involved in responding to an emergency.
Table-top Emergency Response Drills	To familiarize staff with the emergency response process and participants.	Increases efficiency, effectiveness, and interagency cooperation and coordination.	Presents a scenario with key players participating. Advances participants through scenarios; lessons learned are presented.	Consultant; Fire Department; Police; Local Emergency Response Agency	Employees involved in responding to an emergency.
Full-scale Emergency Response Drills	To enhance knowledge and capabilities needed during an emergency response.	Increases efficiency, effectiveness, and interagency cooperation and coordination.	Presents a scenario where the key players are located at their respective agency locations during a mock emergency. Lessons learned are presented.	Consultant; Fire Department; Police; Local Emergency Response Agency	Employees involved in responding to an emergency.
Incident Command System (ICS)	To teach the principles of ICS and to become familiar with the structure and terminology.	Enhances understanding of the ICS, allowing for future participation in an emergency.	Includes modules designed to start with the basic structure of ICS and progress to becoming an Incident Commander and understanding the responsibilities associated with that position.	State or Local Emergency Response Agency	Presidential Directive 5 requirement; employees involved in responding to an emergency.
First Aid/Cardio-Pulmonary Resuscitation (CPR)	To provide care to another person.	Enables assistance for persons when injured prior to emergency care.	Teaches basic first aid to provide initial care to an injured person. Teaches the steps to baby, child, and adult CPR.	The Red Cross; Consultant; Safety Coordinator	Beneficial to have more than one person certified at a utility.
Equipment Use	To understand the operations and limits of a machine.	Prevents potential hazards.	Provides background on how the machine works and a skills test on how to use the equipment.	Vendors; Consultants; Safety Coordinator	For those employees working with specific equipment.
– Fire Extinguisher	To effectively use a fire extinguisher and associate fire types with the proper extinguisher.	Eliminates small fires.	Teaches the parts to an extinguisher and types of extinguishers; practice using an extinguisher on a fire.	Fire Department	

TABLE 2-1
Types of Security and Emergency Response Training Relevant for Water Utility Personnel

Training Type	Purpose	Benefit	Description	Resources to Provide Training	Notes
– On-line Monitoring	To teach use on-line monitoring equipment throughout the water systems.	Enables the utility to know about a contaminant before it reaches the water plant or the distribution system.	Presents the use and maintenance of specific monitoring equipment.	Vendors; Operating Staff; SCADA Operators	For water quality staff, distribution system operators, and treatment plant operators.
– 800 Megahertz (MHz) Radios	To teach the capabilities and operations of a 800 MHz radio.	Ensures effective use of a 800 MHz radio, which police and fire departments use.	Presents the operations, channels, codes, and general maintenance of the radio; practice using a radio.	Local Emergency Planning Agency; Police; Fire Department	Managers or operators assigned to using the radio during an emergency.
– Other Safety Equipment	To learn about other types of safety equipment, and company and Occupational Health and Safety Administration (OSHA) laws.	Prevents a hazard event from occurring by knowing how to use safety equipment properly.	Discusses the various types of equipment that exist (e.g., breathing apparatus), their uses, capabilities, and limitations.	Safety Coordinators	
HAZWOPER (Hazardous Waste Operations and Emergency Response)	To become familiar with hazardous material handling and requirements.	Fulfills federal regulations and prevents hazards from occurring.	Fulfills HAZWOPER training requirements that must be conducted in accordance with Title 29, Code of Federal Regulations, Part 1910.120 (29 CFR 1910.120). This training is required for personnel who handle, ship, or dispose of hazardous materials, or who are assigned to emergency response teams for hazardous materials. Both initial and annual refresher training is required.	Federal Emergency Management Agency (FEMA); Fire Department; Local Emergency Planning Agency; Consultants	Personnel handling hazardous materials.
Cross-Training	To familiarize employees with job responsibilities outside their areas of responsibility.	Provides backup knowledge in the operation of critical facilities.	Provides background information and hands-on training to operate critical facilities.	Utility management	Restrict to critical functions for emergency operations.
General Emergency Management Training	To provide general emergency management courses offered on the FEMA Emergency Management Institute training campus.	Improves coordination during an emergency.	Provides a concentrated emergency training experience.	Held at FEMA's Emergency Management Institute in Emmetsburg, MD (www.training.fema.gov)	Managers and personnel involved in an emergency; funding is available from FEMA and DHS—see the FEMA training web site.
Utility Introduction for Emergency Personnel	To familiarize emergency personnel (e.g., police, fire) with utility facilities	Increases communication and decreases response time during emergencies.	Provides a tour and brief classroom training relative to the utility's system components, normal conditions, chemicals stored onsite, vulnerable points, etc.	Operating staff; consultants.	First responders (e.g., police, fire personnel).

2.6 Records Management

It is critical that utilities have policies in place that specify the documents that are sensitive, and that the utilities manage their documents and records so that sensitive documents remain in a secure environment. These actions are needed to prevent sensitive documents from being accidentally released to the public, for example, in response to a FOIA request. Utilities should consider developing levels of document security ranging from non-sensitive (available to the public without restriction) to highly sensitive (available only to limited staff and maintained in a highly secure environment). Examples of records and material that should be considered as sensitive include:

- Vulnerability assessments, including supporting documents and files
- Emergency response plans and disaster recovery plans
- Audit records related to security
- Security and emergency response training materials
- Plans and specifications for security systems
- Plans and specifications that show the locations of critical assets and security equipment
- Current and historical operating records

Suggested policies for consideration for securing sensitive documents include:

- Providing access to sensitive project materials to authorized staff only.
- Keeping all hardcopies of sensitive material in a locked metal file cabinets to which only authorized project team members have access. Containers with locking bars could be used that are similar to those specified by the federal General Services Administration (GSA) – minimum Class 5 security containers. (See GSA specification AA-F-363D for more information regarding these cabinets.)
- Shredding all discarded working copies and maintaining only the minimum number of hard copies required. Shredding should take place onsite, and should not be contracted to an outside vendor.
- Maintaining all electronic copies of sensitive material on a password-protected secure server. Only authorized staff will be given access to this material. (See Section 5, "Cyber Security Management, Operations, and Design Considerations," for additional information regarding precautions that can be taken to prevent unauthorized access of electronically stored documents.)
- Attaching a confidentiality clause to all sensitive documents given to authorized outside agencies and organizations. This clause can declare that these documents should not be reproduced nor given to others without authorization. The confidentiality clause should be present on all pages of a document, not just the covers.
- Prior to distributing sensitive documents, verify the identification of the recipient and determine whether the need for the document is valid.

- Requiring individuals from outside agencies and organizations who are given access to documents to sign confidentiality agreements.
- Preventing transmission of sensitive material electronically (such as via e-mail and downloading from servers).
- Including a confidentiality notice with electronic correspondence, such as:

> *Confidentiality Notice: This e-mail and any files transmitted with it are confidential and intended for the sole use of the individual(s) to whom they are addressed. If you have received this e-mail in error, please delete the original message from your system and destroy any copies.*

Utilities should consider how information about their facilities is distributed to potential contractors, consultants, and other outside agencies and organizations. Plans, maps, and specifications can serve as roadmaps and planning tools for malevolent actions. To control documents circulated to contractors, all bid documents can be distributed on a CD-ROM (that cannot be duplicated). Requiring a deposit for the CD-ROM can also provide an incentive for unsuccessful bidders to return the documents, which can be destroyed at that time.

Project materials are to be kept confidential at all times on consultant and contractor projects. To keep these materials confidential, a clear project chain of command is identified and followed rigorously so that information is exchanged only as specified. Second, all electronic project working files are isolated in a secure, encrypted project library with access provided only to authorized users with appropriate levels of password protection. Also, periodic security surveys are conducted to determine whether staff, outside agencies, and consultants are following the security procedures.

Because public agencies are subject to state and federal FOIA requests, it is important to have established measures to prevent sensitive documents such as vulnerability assessments or security plans from being subject to public requests. An exemption for security-related information was added to the federal FOIA law and was included in the Public Health Security and Bioterrorism Response Act of 2002, which required community drinking water systems to conduct vulnerability assessments. Because state laws are generally not superseded or limited by federal law, utilities in some states cannot rely on the federal FOIA exemption to protect sensitive information. As such, many states have also included special provisions in their FOIA laws to exempt security-related information. Find out what your state's rules are by consulting your state agency. For a summary of security-related FOIA exemptions, see "Protecting Water System Security Information" by the National Conference of State Legislatures (2003) or "State FOIA Laws: A Guide to Protecting Sensitive Water Security Information" by the AMWA.

Computerized Maintenance Management Systems (CMMSs) and SCADA systems, when fully integrated, offer database compilation of considerable amounts of data pertinent to water system operations. This data, along with the other documents listed at the beginning of this section, contain important information regarding the utility that can be useful in both normal or emergency operating conditions. Electronic databases offer benefits such as automatic backups and other security controls; the policies and practices for managing electronic data should be comparable to those managing the security of business files and other paper documents.

2.7 Policies and Procedures

Simple and effective changes to a utility's policies and procedures can often have just as great an impact on risk reduction as capital improvements or installation of security devices. Policy and procedure changes are generally quick to implement and low in cost, making them an extremely effective way to improve utility security. The key to the success of any change is to make sure that the staff understands and accepts the new policies and procedures. It is imperative that the staff is well informed of the policies and procedures and the reason that these are important. Policies and procedures can only be effective when they are consistently implemented. Some general policy and procedural recommendations provided below.

2.7.1 Basic

- Track keys issued to personnel.
- Retrieve keys when no longer needed, including those instances when personnel are reassigned.
- Replace locks on an as-needed basis to reduce the likelihood of security breaches due to lost keys, unauthorized duplicate keys, keys held by former employees, etc.
- Replace of the traditional key systems with a card reader system for better control options.
- Implement random, but frequent, inspections of the security perimeter at critical facilities identified in the vulnerability assessment and designating appropriate review intervals for inspections of security equipment at other facilities. Establish a minimum number of personnel in the inspection crew in procedures, safety plans, etc.
- Implement a formal annual review of the adequacy of security plans, procedures, and equipment.
- Involve and cooperate with other organizations that can affect the utility's security. For example, contact chlorine and other chemical suppliers to discuss the need for adequate security during transport as well as to develop protocols to respond to missing or delayed shipments.
- Maintain replacement parts and emergency repair kits for critical assets, such as generators, that are important during emergencies. Maintain redundant equipment, critical replacement parts, etc. in a separate or isolated location. It can be on site or nearby, but not within the same building or room.
- Develop a utility vehicle use policy (including locking vehicles and tool bins, securing tools, etc).
- Establish procedures for night shift workers at treatment facilities, including regular check-ins with supervisors.

- Establishing published guidelines so that all future procurements and designs address security issues and incorporate solutions. All requests for proposals should include a security portion so that responding consultants are reminded that security must be addressed in their work and in their own operational practices.
- Continuing to monitor the visitor entrance. Establish a policy for facility tours delineating who is authorized to approve access, areas that can be accessed, and the times that tours are allowed.
- Establish and implement a system of chemical receipt checks as both a safety and security measure. Detailed information on topics such as purchasing, pre-unloading verification, sampling, and testing can be found in the September 2001 issue of *Journal AWWA* in the article titled, "Improved Chemical Handling Procedures."

2.7.2 Advanced

- Compartmentalizing access to various parts of the water system so only necessary personnel are granted access to specific areas. For example, limit access to SCADA cabinets to appropriate personnel.
- Placing alarms at remote facilities into a non-alarm mode for temporary access when authorized entry is made. This temporary mode will automatically revert to a secure mode after a preset time.
  - Program this feature into card-key access systems.
  - Require call-in to alarm station prior to entry for facilities without card-key access.
- Supporting citizen crime-watch committees in areas around utility facilities.
- Establishing a maintenance program to keep alarm equipment, hardware, and fence lines properly maintained. Maintenance of all security equipment, including physical systems such as fences, is a vital part of the security of the water system. Dedicate required resources for proper oversight of the security systems and maintenance program.
- Establishing distribution system contingency plans. Utilities can consider the use of distribution system modeling for emergency response to isolate the distribution system and flush and contain the contamination.
- Maintaining security incident, alarm, and audit logs.
- Ensuring that generators are exercised regularly under realistic loading scenarios so that their reliability is ensured in an emergency.

The following is a list of general policy and procedural recommendations specifically for laboratory facilities:

- Secure laboratory reagents and limit access only to authorized personnel.

- Continue to create and maintain an inventory of reagents kept at the laboratory. Such an inventory would alert the plant manager if someone is buying dangerous chemicals (e.g., metals, cyanide, etc.) each week for a few months and accumulating a large enough quantity to cause serious problems at the plant.
- The laboratory manager should perform random checks to catch unusual patterns of excessive purchase of dangerous chemicals. Currently, scientific chemical suppliers do not have limits on quantities that can be ordered. The laboratory manager should arrange with the suppliers to limit the amount of chemicals that can be ordered at one time. Also, the plant manager should arrange with the chemical vendors to ship only those orders requested by authorized staff.

2.7.3 Suggested Policies

The following checklist can be used as a starting point for developing policies to address security at the utility:

- Human Resource Policies
  - Who is subject to background checks and what checks are made
  - Requirements for employee identification, including badging
  - Protocol for contacting off-duty and on-call employees for emergency response
  - Management succession
- Training Policies
  - Definition of appropriate training
  - System of selecting staff for training
  - Cross-training goals
- Vehicle and Heavy Equipment Policies
  - Definition of authorized use, especially in emergency situations
  - Circumstances under which vehicles and equipment can be taken home
  - How and where vehicles and equipment are to be parked or stored
  - Requirements for locking vehicles and securing equipment
- Facility Access Policies
  - Key, card key, and lock control
  - Limiting access to facilities or portions of facilities by security level
  - Handling of visitors, tour groups, vendors and deliveries, chemicals, construction materials, packages, mail
  - Construction site security
  - Alarm and CCTV monitoring protocols
  - Guard service

- Information Access Policies
  - SCADA
  - Management information system, facilities information system, laboratory information management system, computerized maintenance management system), etc.
  - User name assignment and password protection
  - Internet and intranet use
- Records Management Policies
  - Storage and retrieval of documents
  - Archiving and long-term storage
  - Employee access to FOIA-exempt documents
  - Clear-desk and clear-screen issues
  - Bid plans and specifications
- Materials Management Policies
  - Responsibilities and authorities
  - Inventory frequency
  - Emergency purchasing authorization

2.8 Procurement

For the most efficient response and recovery to an emergency, utilities may want to be familiar with both standard and emergency procurement procedures.

2.8.1 Emergency Procurement

To undertake rapid and effective response to and recovery from catastrophic events, it is imperative for the staff of a water utility under specific circumstances to be able to procure supplies, materials, and services quickly and outside the normal procurement process. Utility managers should familiarize themselves with existing procurement policies to determine whether provisions exist for emergency procurement and, if necessary, proceed with instituting changes that may be needed to address malevolent acts in addition to the natural threats typically covered by procurement regulations.

Emergency procurement of supplies, equipment, materials, even contract labor, are part of and should be detailed in the ERP issued by a utility to ensure business and operational continuity. Section 7, “Emergency Response Planning,” contains additional discussion on ERPs.

Most water utilities have, or are covered by, policies of their parent governments that address emergency procurement; however, these existing policies may not provide the flexibility needed to effectively respond to the types of incidents that utilities may be facing today. Many procurement policies allow for emergency purchases of materials and supplies, and possibly services, through an abbreviated procedure that usually postpones the need for the highest level of approval typically required for purchases. For example, approval of a purchase or an award of a contract that normally

requires governing board approval may be authorized by a utility staff member and brought to the board for an “after-the-fact“ approval once the emergency is over and with the expectation that sufficient justification for the procurement action is required.
Procurement policies may require the declaration of an emergency by an elected official or the highest level of the organization before the standard procurement steps can be waived. Other procurement policies may delegate the authority to make an emergency purchase to a department manager if that manager can justify that the purchase is necessary to immediately protect life, health, and safety that would otherwise be jeopardized if the normal procurement procedures were followed.

While most emergency procurement provisions have met the needs of water utilities over the years, the malevolent acts now being faced create some new challenges that existing procurement policies may not be able to meet. For example, an event may result in injuries, fatalities, and interruptions in both communications and power. It may be impossible for local authorities to declare an emergency condition, or if declared, utility staff may not receive the declaration in a timely manner. Similarly, approval of an emergency procurement by a high-level official may not be possible within the timeframe necessary to react to a life-threatening condition.

Consequently, procurement policies should address emergency purchases that may be necessary under extreme conditions where high-level approvals may not be achievable and where communication networks are out of service. The following provisions should be considered for inclusion in a utility’s procurement policy:

- Allow for the procurement of construction services, engineering services, and personnel services in addition to the purchase of materials, equipment, and supplies.
- Permit emergency procurement to protect imminent harm to the environment and property and maintain water service in addition to the protection of life, health, and safety.
- Authorize emergency procurement to protect “employees“ in addition to the “public“ to avoid ambiguity.
- Eliminate the requirement of an official outside of the utility to declare an emergency as a prerequisite to invoking emergency procurement procedures, and provide a chain of decision-makers authorized to approve emergency purchases. For example, if the Utility Director is unavailable or unreachable, the Water Operations Manager can give approval; if both are unavailable or unreachable, the Maintenance Superintendent may give the approval.
- Authorize approval of emergency procurement to management and supervisory personnel at different locations (facilities) throughout the utility.
- Provide for an automatic waiver of standard procurement procedures should a certain level of threat be declared for the utility’s location by a government agency (e.g., DHS raises the Threat Advisory to “red“).
- Include the need to strive for integrity and fairness in the procurement process, even during emergency situations.

- In addition to making emergency procurement procedures more attuned to the threats faced by water utilities, leverage other procurement methods to provide flexibility to prepare for, react to, and recover from disasters. On-call contracts are an effective method to acquire materials or services as needed without having to go through multiple procurements or invoking emergency purchasing procedures. On-call contracts are procured through normal procedures at annual, biennial, or even 5-year intervals.
- Have contractors and suppliers bid on a "basket" of items or services developed by the utility. More than one contractor or supplier can be selected for the same items or services to allow the greatest flexibility to the utility when the need arises. On-call contracts should require availability of service 24 hours a day, 7 days a week, every day of the year. In selecting a contractor or supplier, balance the need for a quick response that is better met by a company in proximity to the utility with the fact that being in proximity may mean that a company may not be able to respond if a regional catastrophe occurred.
- Use existing contractors to provide immediate availability of equipment and labor to respond to an emergency. Utilities typically have a number of ongoing construction projects as part of their CIP and annual maintenance activities. These existing contracts can be successfully used to quickly bring in construction equipment and expertise to supplement the utilities' workforces.
- Initiate cooperative purchasing agreements to provide increased flexibility for procurement. Cooperative purchasing allows a utility to procure items and services through contracts that exist between other organizations (e.g., other utilities, government agencies, industry associations) and their suppliers and contractors. In most states, municipalities and counties can make purchases from state contracts, and state and local governments can make information technology purchases from federal GSA contracts. Utilities may wish to coordinate with other utilities and local governments in their states and adjacent states and cooperate on developing specifications and allowing purchases from each other's contracts.

2.8.2 Procurement of Security-related Equipment and Services

Utility managers may be concerned about following standard procedures when procuring equipment, materials, and services that relate to the security of assets. The requirement of public advertising for bids on security equipment and projects with detailed plans and specifications may jeopardize the very security being put into place. While states may enact laws exempting security-related documents and drawings containing security information from FOIA requests, at least one state has begun to address this issue of exempting the procurement of security-related materials or projects from the requirement to publicly advertise and receive formal bids. As shown in Figure 2-2, the State of Alabama recently did take such action by amending its State Code to exempt security-related procurements. (Legislative Reference Service of the State of Alabama 2004).

While an exemption from public advertisement and bidding procedures provides a utility the greatest flexibility, there are other methods that may reduce the risk of exposing a utility's security strategy in its process of procuring equipment and construction services. Some steps that may be taken for security-related projects include:

- Allowing for soliciting of price quotes from vendors and contractors without widespread public notice.
- Pre-qualifying contractors, consultants, and suppliers and allowing only those meeting specific criteria to bid on security-related projects.
- Requiring that officers and staff of any company desiring to do security-related business with the utility sign confidentiality agreements.
- Allowing viewing of plans and specifications only within a secure room instead of distributing plans to potential bidders or providing access to a central "plan room."
- Dividing projects so that no one bidder has a complete view of the project.
- Considering design-build contracts where one company is selected to both design and construct the facilities, or in the case of security equipment, both develop the specification and be responsible for its installation.

The Code of Alabama

¶39-2-2(g) "In the event of a proposed public works project acknowledged in writing by the Alabama Homeland Security Department as (i) having a direct impact on the security or safety of persons or facilities and (ii) requiring confidential handling for the protection of such persons or facilities, contracts may be let without public advertisement but with the taking of informal bids otherwise consistent with the requirement of this title and the requirements of maintaining confidentiality. Records of bidding and award shall not be disclosed to the public, and shall remain confidential."

¶41-16-51(a) "….the competitive bidding requirements of this article shall not apply to: …(15)Contractual services and purchases of product related to, or having an impact upon, security plans, procedures, assessments, measures, or systems, or the security of persons, structures, facilities or infrastructures."

Enacted May 2004

FIGURE 2-2
The Code of Alabama

2.9 Communications

When it comes to safety, security, and emergency response, effective communication is the single-most important concept that can assist in repair of a problem and restore public confidence. It is also a concept that is not often initially considered by the technical staff involved in an emergency event.

The benefits of effective communication include increased efficiency, improved coordination to accomplish a goal, and more available resources, such as equipment and technical knowledge, from other agencies. Furthermore, communication improves emergency response efforts by decreasing response times and allowing utilities a sense of confidence based on anticipated assistance from other agencies. Lastly, effective communication can create a sense of teamwork and camaraderie among utility personnel and the outside agency personnel who assist them.

2.9.1 Communications Equipment

Many types of radios and phones can be used to communicate with utility employees or with outside agencies such as the fire department utility management can consider using any of the following options:

- Two-way radios[4] are a highly effective means of standard communication between dispatchers and field vehicles. Extra charged batteries can be carried at all times to prevent loss of contact.
- Cellular phones[4] are becoming more popular, especially those with two-way radios built in. Again, extra batteries and/or a charger should be readily available. Keep in mind that, during large scale emergencies, cell networks can become overloaded and useless, or the repeater towers and equipment are off-line.
- 800 MHz radios are used by fire and police departments; a utility is encouraged to have at least one 800 MHz radio to facilitate communication with first responders. Training is required to understand how to use this technology and communicate with responders. Training is often available through local fire, police, or emergency managers.
- Volunteer Amateur (ham) Radio Operators offer an alternate distance communication channel. Research the capabilities that may be available in your community.
- Government Emergency Telecommunications Service (GETS) Program (http://gets.ncs.gov/) allows utility staff to obtain a telephone line by dialing an access code during an emergency. This line can prove very useful in a situation when telephone and cellular phone lines are typically busy. It is free to sign up and receive calling cards for selected staff. During use, there is a minimal charge per minute. Utilities must sign up for this service prior to the actual emergency or need to use the service.

2.9.2 Internal Communication Practices

Internal communication practices are important in preparing, identifying, and responding to security concerns. Following standardized procedures when communicating with fellow staff during an emergency is extremely valuable. It allows for efficient responses and decreased conversation time, both beneficial during an emergency.

Utility management should provide personnel with a clear protocol for reporting security concerns. This procedure is utility-specific and could simply be a telephone number to the utility manager or a detailed procedure for notifying security staff or police.

Emergency contact lists are essential for contacting staff after hours for emergencies. Many utilities maintain on-call schedules, with associated home, cell phone, and pager numbers. Utilities should ask all personnel required for after hours service to provide an after hours contact number or ask that they be willing to carry a utility cell phone for communication after hours. Contact lists should be reviewed at least every 6 months, and updated as necessary. Managers must be aware of privacy concerns, and they should restrict access to employee personal information to only those with a need to know.

[4] Cell phones and two-way radios should not be used during a bomb threat because their signal may set off the bomb.

Methods of developing internal communication include holding employee meetings, posting weekly newsletters, and conducting internal workshops. External activities, such as company picnics and travel, also promote team building.

2.9.3 External Communication Practices

Prevention and emergency response involve many agencies beyond the water utility. Communication between the utility and outside assistance is crucial both during planning for and responding to an emergency. Initiating communication with outside entities should be addressed during planning phases and should not wait for an actual emergency to begin.

Some benefits of communicating with local emergency service providers, government agencies, and neighboring utilities include:

- Increased efficiency in daily operations and during an emergency
- Increased available resources
- Increased knowledge base
- Smoother coordination and recovery during an emergency

2.9.4 Public Outreach

Public outreach is required for a utility to develop a successful relationship with those it serves. A utility may handle security and emergency response in a technically solid manner, but if the public is not properly informed, then any situation can develop into a disaster.

Under normal conditions, public relation considerations can be necessary when performing day-to-day operations and maintenance, such as installing physical protection. These considerations can include:

- Informing citizens of upcoming work effects
- Gaining public acceptance before installing fencing and lighting in neighborhoods

Citizens need to feel that local government officials are listening to them and taking their concerns into account. Local citizens can be extremely helpful in watching for suspicious activities, as shown in the Citizens Helping in Police Service (CHIPS) program case study (Figure 2-3). To further consider this issue, the measure of confidence that the public has in a utility has much to do with how it communicates during normal times, and not just during emergencies. Maintaining standard methods and regular instances of providing information to the local community can establish expectations of current and valid information from the same source during an emergency. Using neighborhood awareness programs, such as "Neighborhood Watch," can also create a sense of awareness and, thus, confidence in the utility operations, strategy, and agenda.

During an emergency there are other key points to consider, such as when and how to notify the public. This emphasizes the importance of a Public Information Officer (PIO).

The PIO is prepared to interact with local citizens and provide appropriate messages from the utility. It is vital that the person designated to interact with the public and the media be trained to do so. Choose this person before an emergency occurs. To instill confidence during an emergency, use personnel in uniform when TV cameras are present. Having planned messages can provide the public with organized and concise information, also facilitating public confidence.

Distributing information to the community quickly is essential. Waiting until all facts are known may be counter-productive, as news agencies will provide interpretations into the vacuum of information not provided by the local government and utility. Be prompt, frequent, and reliable. A good article regarding public outreach for review concerns the Tylenol poisoning crisis from 1982: "The Tylenol Crisis – How Effective Public Relations Saved Johnson & Johnson," by Tamara Kaplan, Pennsylvania State University (http://www.personal.psu.edu/users/w/x/wxk116/tylenol/crisis.html).

Case Study: CHIPS Program in Kennewick, WA

Citizens Helping in Police Service (CHIPS) is an organization of Citizen Volunteers that has been a part of the Kennewick, Washington Police Department for many years. The CHIPS group is a formally structured non-profit organization with elected officers, regular meeting dates, operational procedures, and designated uniforms. These citizen volunteers, working together with common goals, provide a valuable service to the Department and to the City of Kennewick. The volunteers participate in a number of tasks on a regular basis as well as being an "on-call" group ready to perform tasks on an "as-needed" basis. One of the CHIPS projects, named "Operation Camel," provides a daily physical check of all water storage/pumping facilities in the City of Kennewick.

FIGURE 2-3
Case Study: CHIPS Program in Kennewick, WA

2.10 Interagency Coordination

Part of protecting utility infrastructure involves interaction with other agencies. By reaching out to neighboring utilities, a utility may gain use of equipment and technical resources that lower costs. Coordination with city or county offices such as emergency management agencies (e.g., Local Emergency Planning Committees [LEPCs]) and health departments may open doors for existing equipment, grants, and other assistance that the utility did not previously know existed. Coordination with other major utilities such as electric and telephone companies prior to an emergency can also prove beneficial during an emergency event.

- Think regionally and begin quarterly or monthly meetings regarding coordination, emergency response, and other relevant topics with other utilities in the area.
- Invite police and fire to have a tour of facilities; learn to use their 800 MHz radios.
- Share telephone lists with key outside agencies; minimally, provide a single point of contact for all agencies that may be involved in a security problem or emergency response action for the utility to use during an emergency.
- Attend training workshops with other agencies and intermix employees so their primary interactions are with people outside of their daily work environment.
- Hold emergency response exercises and invite external agencies to attend.

Prior to an incident, it is important to have mutual aid agreements in place with other utilities and agencies. These agreements often save time, money, and confusion and should address:

- Interconnection with other water systems, if possible (with established rates and charges)
- Sharing of laboratory facilities and resources (with established rates and charges)
- Borrowing of supplies and materials (with the understanding that the borrowing utility will replace the materials with like materials after the emergency is over)
- Borrowing of personnel and heavy equipment (with established rates and charges)

Not all interagency coordination should be performed locally because a large-scale disaster may render local utilities and public works agencies unable to respond. Therefore, some coordination and agreements should be established with utilities and agencies several hundreds of miles away.