SECTION 2

# Managing for Reducing Risks

## 2.1 Introduction

Many of the lowest-cost and highest-value measures that a wastewater utility can take to reduce the risks associated with malevolent actions are cultural changes within the organization, employee training, stakeholder awareness, and policies and procedures that change business practices to help to ensure a more secure workplace and safer facilities. 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 of these low-cost actions, rather than being frustrated by the inability to fund major infrastructure countermeasures.

This section provides concepts, strategies, and actions that wastewater utility managers should consider when contemplating how to better prepare for both known and unknown challenges that may arise.

## 2.2 Governing Body

The governing body of a wastewater utility, whether composed of elected or appointed persons, makes policy and holds the ultimate responsibility to the utility's customers by ensuring proper management of the wastewater system, including maintaining public health and protecting the environment. From this standpoint alone, it is important for utility management to provide governing body members with at least a high-level overview of wastewater system threats and vulnerabilities, and management's approach to mitigating the associated risks to the system. However, because it is likely that governing body 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 on wastewater security.

Possibly the biggest obstacle to implementing security measures will be convincing the governing body that wastewater systems are indeed vulnerable. Utility managers might find the following suggestions to be helpful for their discussions with governing body members:

- Reference *The 9/11 Commission Report* that cites imagination as one of the failures revealed by the terrorist attacks.[9]
- Have the local police chief or sheriff gain a through understanding of the wastewater system, its vulnerabilities, and the consequences that may result from a catastrophic event, and have that law enforcement officer assist in the utility manager's briefing.

[9] *The 9/11 Commission Report*, National Commission on Terrorist Attacks Upon the United States, 2004

- Describe the federal government's National Infrastructure Protection Plan for the water sector and the development of tools and guides by WEF, Water Environment Research Foundation (WERF), and AMSA to assist in the assessment of wastewater system vulnerabilities and in the reduction of security-related risks.
- Use factual occurrences as examples—illegal dumping into a manhole that could have been gasoline instead of septage, or vandalism at a remote pump station that could have resulted in sewage overflows—to emphasize the importance of wastewater system security.
- Clearly show how a security breach can impact public health, damage the environment, and place utility employees at risk.
- Examine the effect of an incident for which the utility was unprepared on the credibility of the utility and the governing body.
- 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 body with more than just the consequences; provide management's approach to responding to the challenges by realistically forecasting short- and long-term needs and their impact on resources (such as labor costs, other operation and maintenance [O&M] costs, and capital) as well as on developing funding alternatives.

While communication with the utility's governing body is imperative, utility managers must be cautious about the security details that might be revealed in public forums. Therefore, discussions about wastewater security with governing body members should be held privately if state and local laws allow. These laws, sometimes known as sunshine laws, stipulate the type of discussions that can take place with board members outside of public meetings and how many governing body members can meet without public notification. Because sunshine laws vary from state to state, utility managers should seek guidance from their legal counsels to ensure that the 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 governing body members were briefed before the meeting, long, detailed discussions should not be necessary.

## 2.3 Customers and Other External Stakeholders

It is unlikely that wastewater systems are high on the list of public security concerns. Nevertheless, utility managers should be prepared to respond to questions from customers, the media, and other external stakeholders who may want to know if or why wastewater security is an issue and what the utility is doing to reduce risks to infrastructure, persons, and service. External stakeholders may include community organizations and environmental activists who are interested in the countermeasures that the utility may have to prevent or mitigate the effects of a chemical release, disruption of service, and the pass-through of dangerous substances through the treatment facility and into receiving waters or reclaimed water systems. 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 natural or malevolent 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, the utility should initiate discussions about wastewater security with a few categories of external stakeholders to improve the planning and implementation of countermeasures and emergency response.

Reclaimed water customers are one category of external stakeholders that need to be briefed on the risks associated with wastewater system vulnerabilities that might result in a change in reclaimed water quality. Likewise, these customers should also be provided with an overview of the steps that utility has taken to prevent contaminated effluent from being pumped into the reclaimed water system, as well as guidance as to whether an alternative supply is available for cooling water, irrigation, or other critical uses if the reclaimed water supply must be suspended.

Wastewater utility managers should also initiate discussions with wholesale customers—those cities, counties or companies that operate satellite wastewater collection systems that discharge into the utility's system. Utility managers should insist, or at least strongly encourage, that these wholesale customers to protect their collection systems with the same level of security as the utility is protecting its own collection system. Any new or renewed wholesale agreements should include requirements for the wholesale customer to institute countermeasures to mitigate risk to the utility's wastewater system.

Implementation of security measures is likely to have substantial impacts on wastewater system budgets, both capital and operating. Whether the utility will fund security projects from debt sources or net revenue, pressure on wastewater rates may necessitate a rate increase. Thus, utility managers may need to inform customers of the importance of security measures to providing uninterrupted service and protection of public health and the environment, without revealing significant details about the approach to security or specific countermeasures. Wastewater utilities may want to consider a specific surcharge on the base wastewater rate to fund security projects. A security surcharge was successfully implemented by the City of Atlanta's Department of Watershed Management in 2004.[10]

**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

[10] City of Atlanta – Ordinance 03-O-2212

Utility managers should discuss the seriousness and sensitivity of wastewater system security with union leaders. Such communication can lead to a more unified approach to security among management and labor, and may help in identifying threats more apparent to employees than to management.

Proactive communications with other wastewater utilities, regulatory agencies, and first responders are also important to developing and maintaining a secure system, as described in Section 2.10.

# 2.4 Human Resources

While policies, operational procedures, and security equipment are important aspects of securing wastewater utilities, these items will have little effect if utility personnel are not aware of and concerned about their roles in ensuring utility security.

## 2.4.1 Organizational Culture

Every organization has a culture that drives employee behavior, guides decisions, affects productivity, and influences how the organization is perceived from both inside and outside. Over the past several decades, wastewater utilities have worked diligently on instilling safety and environmental stewardship as core values of their organizational culture. More recently, many wastewater utilities have also cultivated a sense of efficiency and customer satisfaction into their organizational culture. Now, with the threats faced by all public infrastructure sectors, it is imperative that wastewater utilities also introduce security into the culture of the organization.

Employees are "insiders;" they have unique knowledge of the wastewater system's infrastructure, processes, and vulnerabilities. They are authorized to access both facilities and information, and they are located throughout the utility's service area. Thus, employees can provide a vital role in ensuring that the wastewater system is kept secure through heightened awareness and adherence to policies and procedures. To gain employee buy-in, a good place to begin is with security awareness training for all employees. This training should provide an overview of the vulnerabilities faced by wastewater utilities and the threats against which the utility must be protected. Employees should be provided with an explanation of new and proposed security policies and should be instructed on how they can assist in reducing security risks.

To ensure security concepts are integrated into the organizational culture, utility management must also emphasize security in all its actions and communications. Some suggestions include:

- Discussing security with the staff during formal and informal meetings.
- Making security an agenda item at every staff meeting.
- Ensuring that employees receive adequate security training (see Section 2.5).
- Developing security policies and procedures and enforcing them consistently and equitably.
- Creating a position of utility security officer, or expand the responsibilities and authority of an existing position (e.g., safety officer).

- Ensuring that the individual(s) assigned responsibility for security are also provided the appropriate authority to correct shortcomings and take necessary actions.
- Including articles on security in internal newsletters.

While employees can provide valuable security improvements throughout a utility, as "insiders" they can also prove a great threat if their access to facilities and information is used with malicious intent. Consequently, wastewater utility managers should take measures to mitigate the risks posed by new employees, existing employees, and former employees. However, there are numerous federal, state, and local laws that pertain to employee rights and the employer-employee relationship that will determine the security measures that can and cannot be taken when employees are involved, and when hiring or terminating employees. In addition, bargaining unit agreements will undoubtedly address employer-employee relations and may restrict the employer's use of otherwise lawful security measures. Therefore, it is imperative that the utility's legal counsel be consulted before any security measures involving employees, including those discussed below, are implemented.

## 2.4.2 Background Checks

Basic background checks of applicants for utility positions should be standard practice. At a minimum, such background checks should 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 any job offers are made. If lawful, and if consistent with bargaining unit agreements, background checks with periodic reviews, should also be conducted for current employees, especially upon promotion to a position with fiscal responsibilities.

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. However, there may be significant legal restrictions and liability associated with such enhanced background checks. Whatever level of background checks is conducted, it is imperative that the utility maintains consistency for all applicants or for all those who apply for specific positions.

It should be noted that criminal background checks are sometimes incomplete or erroneous and may need to be confirmed through other channels, if possible. 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 were input specifically into the national system. Similarly, credit records may be both incomplete and inaccurate.

Utility managers should consult with their local law enforcement agencies to determine the most reliable method for obtaining the background checks for applicants and, if appropriate, employees.

Frequently, local law enforcement officials will provide the background check service at minimal cost, or assist the utility in finding a reasonably priced and dependable service provider. However, the utility manager is reminded to seek advice from legal counsel before proceeding with any background checks.

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."[11]

## 2.4.3 Identification Badges

Employee identification (ID) badges provide instant verification of whether individuals are authorized to enter, unescorted, a utility's facility or handle utility equipment. Regardless of how few workers a utility employs, ID badges should be provided. Smaller utilities can have custom photo ID badges produced for less than $10 dollars each plus a one-time setup charge of less than $100.

- All employees, including temporary and part-time employees, interns, and volunteers should be issued photo ID badges.
- ID badges should be worn at all times while working at utility facilities and utility job sites. The badges should be worn above the waist so that they are visible whether the person is sitting or standing.
- Office employees may use a clip to secure their badges or hang them from a lanyard around their neck as long as the lanyard is equipped with a snaphook release to prevent choking if the tag gets caught.
- Field employees should secure their ID badges by wearing them in a protective see-through pouch sewn into their uniform shirt.
- Color-coded badges can be used to alert others if employees are in an area that they are not approved to be in and can deter employees from straying into restricted areas.
- ID badges should contain an up-to-date color photo of the employee, along with an expiration date. Both the photo and date of expiration, and color-code if used, should be visible from a distance of several feet.
- Should the appearance of an employee dramatically change, a new ID badge with an updated photo should be issued.
- ID badges should expire no more that 2 years after the date of issue. Temporary employees, interns, and probationary employees should be issued ID badges with expiration dates that correspond to the projected end of their employment or probationary period.

**Multiple Benefits**

In addition to increasing accountability and improving security, photo ID badges can also help new employees get to know each other's names.

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

- If resources permit, ID badges may contain security features such as holograms, watermarks, magnetic strips, or radio frequency identification (RFID) devices that permit access to designated areas and track locations of employees. See Section 6.3.3 for more information on this type of ID device.
- Employees who forget their badges or are visiting locations where they are not authorized to be as part of their normal duties 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 indicated by an obvious change in their color. Time-sensitive and light-sensitive badges are available for less than $0.25 each. In addition or as an alternative, authorized personnel may escort employees visiting locations outside of their authorized area.

## 2.4.4 Employee Surveillance

Enhanced awareness by all employees is important to reducing security vulnerabilities in the workplace. Security training should instruct employees on the type of activities that should raise concern and how they should respond. Some utilities have taken a low-cost 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 entry readers. Biometrics and RFID devices can also be used to track employees' whereabouts (see Section 6.3.3). "Man-down" alarms, which require an operator to confirm his location by pressing a button or calling an operator in specified intervals, can also reduce the risk of workplace vulnerabilities while improving employee safety. This can be particularly important on overnight shifts or other situations in which only one operator is present.

**Multiple Benefits**

Techniques that monitor employees' whereabouts improve their safety while reducing the risk from insider attacks.

Supervisors should be taught the types of employee behavior that may indicate a threat to the organization or other employees. However, monitoring of employee activities at their workplace may be subject to federal and state privacy laws, as well as bargaining unit agreements. In general, it is acceptable to routinely monitor employee use of electronic media, such as e-mail and Internet surfing. Monitoring of employees through closed-circuit television (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 this policy.

## 2.4.5 Employee Response

Effective reaction to, and recovery from, natural or malevolent events depends upon a rapid and thorough response by a knowledgeable and experienced workforce. Emergency response is explored further in Section 7. Utility management should work with its staff to develop policies and contingency plans to address problems that employees may have traveling to utility sites and

facilities during and after an incident. Staging areas and employee reporting procedures (e.g., roll call by radio or telephone) should be established.

Management should also be cognizant 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. Such an employee-centric and family-friendly approach is critical to achieving buy-in from employees who would be facing tough decisions in a catastrophe.

Human resource policies should address the excuses that will be considered acceptable for an employee not responding to work during an incident or if a severe terrorist advisory is declared, and the action that will be taken for non-excused absences. It is important to note that such policies should be created and applied with a thorough understanding of the utility's legal responsibilities governing employee leave, including relief allowed employees under the Americans with Disabilities Act.

Additionally, consideration should be given to storing several day's supply of non-perishable food along with bottled water should a facility lock-down (employees not being allowed to leave a facility) be necessary. Unused food and water can be donated to a food bank at the end of every year.

## 2.4.6 Contractors

It is important that utility managers consider not only their own employees as a potential insider threat, but also contractors (including engineers and manufacturer representatives and others) who may have access to utility facilities and information at any given time.

Suggested contractor security procedures include:

- Establishing an effective sign-in and sign-out procedure (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 they are easily identified. All visitor badges should be returned at the end of the day.
- Requiring escorts if physical barriers are not present.
- Limiting use of private vehicles on the construction site.
- Evaluating the environmental, health, and safety record of contractors before signing contracts and considering offering environmental health and safety training to contractors onsite.
- Issuing "contractor" ID badges that are returned upon the completion of the contractor's work.
- Performing background checks on contractor personnel assigned to project sites. While this is sometimes a difficult activity, it should be considered depending on the situation.
- Limiting access to sensitive areas (such as chlorine, ammonia, and SCADA).

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 the heavy equipment each night.
- Considering additional fencing and separate entrance, separate parking areas, and guards to coordinate construction staff.

# 2.5 Training

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

## 2.5.1 Types of Training Sessions

Exhibit 2-1 lists training relevant to all wastewater and stormwater utility personnel. If a particular training is more critical for one group of personnel, the group is listed in the Notes column. Training that is associated with emergency response (e.g., table-top exercises and incident command systems) is discussed further in Section 7.6.

## 2.5.2 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 local police and fire departments, local emergency planning agencies, local health departments, and the Red Cross to inquire about available training. Also, nearby utilities may want to share in training sessions and contribute funding.

## 2.5.3 Cross-training

Training staff members in skills outside of their normal duties may be prudent so that more staff are available to 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 and pump station operations. A cross-training program should involve treatment plant workers spending time with and learning the skills of collection system workers, as well as gaining knowledge of the system's pump stations. This type of program also provides a more flexible

**Multiple Benefits**

A staff that is cross-trained in more than one skill will increase operational efficiency through a more flexible workforce by reducing down-time and the need to reschedule staff. Cross-training also prepares a utility for succession as employees leave or retire.

**EXHIBIT 2-1**

Types of Security and Emergency Response Training Relevant for 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 and Document Threats | To assist the public in a calm and effective manner; to more effectively manage employees; to understand threat documentation procedures. | 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; introduces threat documentation forms; practices sample 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. | Consists of a walk-through of the sections; reviews location of information. | City/County 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 scenario with each of the necessary key players involved participating. Advances participants through the scenario; 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 during an emergency response. | Increases efficiency, effectiveness, and interagency cooperation and coordination. | Presents 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 learn the principles of the ICS and to acquaint the staff 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 up to becoming an Incident Commander and the responsibilities associated with that position. | State or Local Emergency Response Agency. | Presidential Directive 5 requirement; employees involved in responding to an emergency. |

**EXHIBIT 2-1**

Types of Security and Emergency Response Training Relevant for Utility Personnel

| Training Type | Purpose | Benefit | Description | Resources to Provide Training | Notes |
|---|---|---|---|---|---|
| First Aid/Cardio-Pulmonary Resuscitation (CPR) | To provide care to another person. | Assists another person when injured prior to emergency care. | Teaches the steps to baby, child, and adult CPR. Learn basic first aid to provide initial care to an injured person. | The Red Cross; Consultant; City/County 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; City 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. | Extinguishes a small fire. | Teaches the parts of an extinguisher and types of extinguishers; practice using an extinguisher on a fire. | Fire Department. | Required by the Occupational Safety and Health Administration (OSHA) to be conducted yearly |
| - On-line Monitoring | To use on-line monitoring equipment throughout the system. | Alerts staff to a contaminant before it reaches the wastewater plant or the receiving water body. | Teaches use and maintenance of specific monitoring equipment. | Vendors; Operating Staff; SCADA Operators. | For water quality staff and treatment plant operators. |
| - 800 megahertz (MHz) Radios | To know the capabilities and operations of an 800 MHz radio. | Teaches effective use of a 800 MHz radio, which police and fire use. | Teaches the operations, channel, code, 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 teach how to use other types of safety equipment, company and OSHA laws. | Prevents a hazard from occurring by properly knowing how to use safety equipment. | Teaches various types of equipment that exist, their uses, capabilities, and limitations (e.g., breathing apparatus). | City and County Safety Coordinators. | |
| HAZWOPER (Hazardous Waste Operations and Emergency Response) | To familiarize staff with hazardous material handling and requirements. | Fulfills federal regulations and prevents hazards from occurring. | Fulfills HAZWOPER training required under 29CFR1910 for personnel who handle, ship, or dispose of hazardous materials, or who are assigned to emergency response teams for hazardous materials. Initial and annual training is required. | FEMA; Fire Department; Local Emergency Planning Agency; Consultants. | Personnel handling hazardous materials. |
| General Emergency Management Training | To provide general emergency management courses offered on FEMA's Emergency Management Institute training campus. | Improves coordination during an emergency. | Provides a concentrated emergency training experience. | Held at FEMA's Emergency Management Institute and Training Facility in Emmitsburg, 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. |

**EXHIBIT 2-1**

Types of Security and Emergency Response Training Relevant for Utility Personnel

| Training Type | Purpose | Benefit | Description | Resources to Provide Training | Notes |
|---|---|---|---|---|---|
| Utility Introduction for Emergency Personnel | To familiarize emergency personnel (e.g., police, fire) with utility facilities. | Increases communication and decreases response time during an emergency. | 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 and fire personnel). |
| Cross-Training | To familiarize employees with job responsibilities outside their areas of responsibility. | Provides backup knowledge in operation of critical facilities. | Provides background information and hands-on training to operate critical facilities. | Utility management. | Restrict to critical functions for emergency operations. |

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 should involve the utility's bargaining union and human resource professionals.

### 2.5.4 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:

- Certification toward professional development hours
- Favorable employee evaluations
- Further career goals/personal development
- Lunch provided during a training session

## 2.6 Financial Considerations

When looking to improve security, financial considerations are critical to successfully reducing risks. Key areas, which are described in more detail in the remainder of this section, include developing Capital Improvement Plan (CIP) programs that adequately support security needs. To sufficiently fund security programs, utilities must develop a diversified strategy for funding both capital and operating needs that decision-making bodies and customers can support.

- Developing funding programs to support operating fund needs.
- Developing funding programs that decision-making bodies and customers can support.
- Developing a diversified strategy for funding both capital and operating needs.
- Integrating Government Accounting Standards Board Statement 34 (GASB 34) considerations with the CIP for security and reporting purposes. (See www.gasb.org for latest requirement details.)

### 2.6.1 Developing CIP Programs that Adequately Support Security Needs

To accomplish security objectives, wastewater utilities need to sustain existing facilities at a functioning level. In addition, they may need to build additional facilities that have been identified through vulnerability assessments and other related evaluations as key to improving security. The measures to improve security take a variety of forms, such as providing redundancy where it currently may not exist, improving the flexibility and management of existing facilities, and securing access to critical facilities.

Having an adequate CIP and funding program is essential because security-related projects often compete with other capital projects, such as:

- **System growth requirements.** Many wastewater systems with growing and developing population bases need to spend substantial funding on capital projects that expand treatment capacity or extend collection system networks to new areas.
- **Correcting 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.
- **Regulatory mandates.** Wastewater utilities must comply with new regulations promulgated by the EPA and state regulatory agencies, as well as specific permit conditions that may require capital investments in new equipment or facility upgrades.
- **Renewal and replacement.** Well-managed wastewater 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 wastewater utilities to have sound processes for identifying, prioritizing, and implementing their capital improvement plans. Traditionally, many wastewater 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, e.g., an asset management approach where risks associated with security vulnerabilities are ranked on the same scale as risks associated with infrastructure failure, regulatory non-compliance, and the inability to meet service levels. Projects that reduce risks are ranked in order of the greatest risk reduction per unit cost.

Another systematic approach to ranking projects is to identify and weigh criteria, then explicitly "score" the performance of candidate projects. In such systems, security considerations could be explicitly recognized as criteria and weighed in relation to other competing priorities. Cost-benefit relationships can then be developed. In this way, the decision-making process considers 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. *The Capital Planning Strategy Manual*[12] includes instructions and tools for implementing such methodology.

[12] American Water Works Association Research Foundation (AwwaRF) and AWWA, 2001

## 2.6.2 Developing Funding Programs to Support Operating Fund Needs

Developing a funding program that supports the operating funds of a wastewater utility is also critical to reducing risks related to security. Defining and securing stakeholder and governing body 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 wastewater utility's assets. Inadequate labor budgets present several labor-related risk threats, including:

- Possibility of facility breakdowns (e.g., a break in a major collection 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 threats to security.

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 running in proper working order.

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

- **Operating reserves.** It is suggested that a minimum of 45 to 60 days' worth of the operating budget needs to be set aside in reserve so that utilities can make payments required to stay in business in the event of a crisis. In some cases, as much as 90 to 120 days' worth of operating budget is needed, especially if revenues are received semiannually or annually via property tax billing, or if an interruption in mail service delays receipt of customer payments by the billing agency.
- **Contingency account.** Consider annual funding of a contingency line-item in the operating budget that would provide for the payment for costs incurred during an emergency (e.g., overtime, contractor services, tanker truck rental, hauling services, and other incident-related response actions).
- **Petty cash.** Cash on hand is needed to support immediate needs for funding emergency activities or to allow transactions with customers or vendors that do not have access to alternate payment tools such as credit cards for purchasing minor equipment and supplies.
- **Debt service coverage.** Many wastewater utilities fund at least a portion of their capital programs through municipal bonds or state revolving fund (SRF) loans. In most cases, these funding vehicles require that net revenues for the utility be adequate to provide some level of coverage (typically between 1.10 and 1.25) above the annual debt service payments. For utilities with substantial outstanding debt, the coverage amount can represent millions of dollars. Wastewater

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 also maintain specific minimum amounts in reserve accounts such as debt service reserve funds and emergency reserve funds.

## 2.6.3 Developing a Funding Program that Governing Bodies and Customers Can Support

In addition to developing budgets that reasonably support the capital and operating funds needed to improve security, wastewater utilities need to develop budgets and funding programs that their governing bodies and customers will support. To gain support from governing bodies, utility management increasingly needs 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 2.6.1, "Developing CIP Programs that Adequately Support Security Needs," above).
- Proposed rate and fee structures are equitable and supportable.
- Proposed financing plans for capital program are optimal. For example, governing bodies increasingly want an evaluation of several financial planning scenarios (e.g., level of bonding vs. equity funding, level debt structure vs. balloon payments toward the end) to ensure that the selected path is consistent with the utility's goals and objectives.
- Adequate outreach to all segments of the customer base regarding any proposed rate increases or changes in the rate and fee structures has been performed.

Governing bodies increasingly want to see the value proposition in their 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.

**Multiple Benefits**

Developing a sound justification for capital expenditures and a financing plan that earns buy-in from a utility's governing body is just good business practice. Following these steps leads to ease of implementation, not only for security projects, but for an overall CIP program.

Customers and other stakeholders are increasingly sophisticated in their attention and interest in wastewater 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.

### 2.6.4 Funding Sources

Many sources exist that can provide grants and loans to utilities to assist in security and emergency response needs. Federal monies are typically funneled through state agencies, often to regions. For example, funding is available from Department of Homeland Security and FEMA through state emergency management agencies. In years past, emergency management funding was typically awarded to first responders; today, utilities across the country are part of this funding. It is prudent for a utility to contact its regional emergency management agency to discuss emergency and security needs and to inquire about available funding.

The following list provides sources of grants and loans that may be available. Note that for FEMA funds, utilities would have to apply through their associated state agency.

**Small Utility Tip**

Hardships Grants Program for Rural Communities (HGP) provides assistance to communities with populations of 3,000 or less at http://www.epa.gov/owm.

- The Pre-Disaster Mitigation Program (PDMP) (www.fema.gov/fima/pdm.shtm).
- Multi-Hazard Mitigation and Terrorism Prevention (MHMTP) (www.fema.gov/library/prepandprev.shtm#multi).
- The Hazard Mitigation Grant Program (HMGP) assists states and local communities in implementing long-term hazard mitigation measures following a major disaster declaration (www.fema.gov/fima/hmgp).
- Clean Water State Revolving Fund (CWSRF) programs provided about $4 billion annually in recent years to fund water quality protection projects for wastewater treatment, non-point source pollution control, and watershed and estuary management. States may also provide loans for security related improvements through the CWSRF (www.epa.gov/owmitnet/cwfinance/cwsrf/index.htm).

Additional information on funding can be found in the Catalog of Federal Domestic Assistance (CDFA) at www.cfda.gov.

## 2.7 Records Management

Our society's thirst for information, as well as the ease of transmitting and duplicating that information in this technological age, makes it extremely challenging for utilities to control sensitive documents. Since September 11, 2001, there has been an increasing understanding of the need to manage sensitive information, but, as with many areas discussed in this document, it is still a balancing act between convenience and security. It is often necessary to distribute documents, both internally and externally, but there are steps that can be taken to maintain better control.

Utilities should recognize that plans, maps, and specifications can serve as roadmaps and planning tools for potential adversaries. To maintain the security of their systems, it is critical that utilities have policies in place that specify the documents that should be declared sensitive, and that utilities manage their documents and records so that sensitive documents remain in a secure environment.

Utilities should consider developing levels of document security ranging from documents that are non-sensitive and available to the public without restriction to those that are highly sensitive and should be available only to limited staff and maintained in a highly secure environment. Examples of records and material that may be considered sensitive include:

- Vulnerability assessments, including all 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
- Security incident reports
- Engineering record plans and specifications of treatment plants, pump stations, collection system sewers and other collection system facilities
- O&M manuals
- Personnel records

Recommendations for securing sensitive documents include:

- Providing access to sensitive project materials to authorized staff only.
- Preventing transmission of sensitive material electronically (e.g., via e-mail and downloading from servers). For information that must be transmitted electronically, include a confidentiality notice, 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.*

- Maintaining all electronic copies of sensitive material on a password-protected secure server, and allowing only authorized staff to have access to this folder. (See Section 5, "Cyber Security," for additional information regarding the precautions that should be taken to prevent unauthorized access of electronically stored documents.)
- Carefully monitoring information that is put on public web sites. As part of community outreach, it has been common for utility maps and facility information to be available on web sites, but this produces a security risk. If the utility's information is included on a municipal web site, coordinate with the municipality staff to ensure that sensitive information is not publicly available.
- Requiring management authorization or approval to publish information on public notices, web sites, and flyers.
- Shredding all discarded working copies (subject to state and local laws) and maintain only the minimum number of hard copies required. Shredding should take place onsite and should not be contracted to an outside vendor.

- Keeping all hardcopies of sensitive material in locked metal file cabinets with locking bars such as those specified by the Federal General Services Administration [GSA] – minimum Class 5 security containers. (See GSA specification AA-F-363D for more information.) Only authorized project team members should have access to these containers.
- Storing and retrieving documents.
- Archiving and storing documents long-term.
- Implementing clear-desk and clear-screen policies.
- Segmenting documents to allow wider distribution of non-sensitive information, while sensitive portions are restricted authorized staff only. For instance, engineers who need information from the utility's VA to procure and specify equipment for security improvements may not need to view the entire VA. Allow only designated individuals to view the entire VA and give other staff members only the portions needed to do their jobs.

Utilities should consider how information about their facilities is distributed to potential contractors, consultants, and other outside agencies and organizations. Recommendations for securing documents in these instances include:

- Limiting the general information provided in contract drawings and specifications to the minimum required to produce an adequate bid. Other information can be provided on a need-to-know basis once a contract is awarded.
- When it is necessary to give sensitive documents to contractors, regulators, and outside agencies, attaching a confidentiality clause that declares that 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, verifying the identification of the recipient and determine whether the need for the document is valid.

To ensure that project materials are kept confidential at all times on consultant and contractor projects, a clear project chain of command that is followed rigorously can help to ensure that information is exchanged only as specified. Consider isolating all electronic project working files in a secure, encrypted project library with access provided only to authorized users with appropriate levels of password protection. Also, periodic security surveys can help to ensure that all internal staff and external agencies and consultants are following the security procedures.

Regulatory agencies also hold a large amount of information on wastewater utilities through the compliance reports and documents they require. Utilities should schedule a meeting with state regulatory agencies so that they are aware of the information that the regulatory entity will hold confidential and what will be released to the public. This information will assist utilities in determining the depth of the information they submit (within their control) and also educate the regulators on the potential sensitivity of the information.

Because public agencies are subject to laws such as the federal Freedom of Information Act (FOIA) and state public records acts, it is important to establish measures to prevent sensitive documents such as VAs 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 water utilities 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. Many states have added special provisions into their laws to exempt security-related information. Utilities should contact the appropriate state agency to learn about state rules regarding public records. A summary of security-related FOIA and state public records act exemptions can be found in "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 Association of Metropolitan Water Agencies (AMWA).

Finally, it is imperative that all information critical for effectively responding to emergency situations and for rapidly recovering from disasters be maintained in both hardcopy and electronic format. When power is interrupted and battery supplies on laptops expire, a hardcopy of important documents must be available. On the other hand, should a malevolent event result in paper documents being destroyed or unusable, electronic copies will be invaluable.

## 2.8 Policies and Procedures

Simple changes in policies and procedures at a utility 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 such change is to make sure that the staff understands and accepts the new policies and procedures. While the development of utility policies is well within the purview of management, consideration should be given to having employee teams develop procedures that supports and complements the policies. This type of employee involvement can encourage staff buy-in. It is also important to remember that policies or procedures can only be effective if they are well known to the staff and that they are consistently and fairly implemented.

The following is a partial list of policies that can be developed to improve security within the utility.

- 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 (see also Section 3)
  - 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 (see also Section 5)
  - SCADA
  - Management information system, laboratory information management system, computerized maintenance management system, financial information system, etc.
  - User name assignment and password protection
  - Internet and intranet use
- Materials Management Policies
  - Responsibilities and authorities
  - Inventory frequency
  - Emergency purchasing authorization

The content of the policies should be decided based on the DBT determined from a utility's VA and the information presented throughout this document. Utility policies, and the procedures that support them, should be tied to the U.S. Department of Homeland Security's Threat Advisory System (or similar state system) so that more stringent security measures are put in place as the threat condition (i.e., green, blue, yellow, orange, red) increases.

Examples of policies can be found in the document entitled, *Site Security Guidelines for the U.S. Chemical Industry*.[13]

## 2.9 Procurement

The procurement of equipment and services can involve complex policies and procedures to assure open competition and transparent processes. Such policies and procedures can be especially burdensome under the stress and time constraints of a security incident or other emergency. Requirements for public solicitation of bids may potentially jeopardize a utility's security when such solicitation is for security equipment or security-related construction. Consequently, utility managers should consider adopting policies that will facilitate procurement under emergency situations and provide confidentiality of security measures to be employed by the utility.

[13] Site Security Guidelines for the U.S. Chemical Industry. the American Chemistry Council, the Synthetic Organic Chemical Manufacturers Association, and The Chlorine Institute, Inc., 2001.

## 2.9.1 Emergency Procurement

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

Many wastewater utilities 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 body 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 wastewater utilities over the years, the malevolent threats 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 even 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. Consideration should be given to including the following provisions 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 to maintain wastewater service in addition to the protection of life, health, and safety.

- Authorize emergency procurement to protect "employees" in addition to the "public" to avoid any 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's director is unavailable or unreachable, the wastewater operations manager may give the 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., the Department of Homeland Security raising 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 wastewater utilities, other procurement methods should be leveraged 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. 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, consideration should be given to balancing 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 has occurred.

Utilities may want to consider using existing contractors to provide immediately available equipment and labor to respond to an emergency. Utilities may have a number of ongoing construction projects as part of their CIP and annual maintenance activities. These existing contracts can be used to quickly bring in construction equipment and expertise to supplement the utilities' workforces.

Cooperative purchasing agreements also 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 all 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.

## 2.9.2 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 for security equipment and projects with detailed plans and specifications may jeopardize the very security being put into place. While several states have enacted laws exempting security-related documents and drawings containing security information from FOIA or public records requests, at least one state has addressed this issue. The State of Alabama recently did take such action by amending its State Code to exempt security-related procurements.[14]

While an exemption from public advertisement and bidding procedures provides utilities with the greatest flexibility, there are 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:

- Raising the level at which public advertisement and formal bids are required, thus 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 signing of confidentiality agreements by the officers and staff of any company desiring to do security-related business with the utility.
- Requiring background checks for any contractor personnel working onsite.
- Allowing viewing of plans and specifications only within a secure room or a central "plan-room" instead of distributing plans to potential bidders.
- 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

[14] Legislative Reference Service of the State of Alabama, 2004

# 2.10 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, effective 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.

## 2.10.1 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 and 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. However, managers must be aware of privacy concerns; 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. Any contact list should be reviewed regularly, at least every 6 months, and updated as necessary.

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

## 2.10.2 External Communication Practices

Emergency prevention and response involve many agencies beyond the utility. Communication between utilities and outside assistance is crucial both during planning for and responding to an emergency. Communication should be addressed immediately during planning phases and should not wait for an actual emergency to begin.

Some benefits of communicating with local emergency service providers (e.g., police and fire-rescue), 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

It is important to include an emergency contact list in the utility emergency response plan, and check the telephone numbers at least every six months. See Section 7.4 for suggestions regarding the contacts to include.

## 2.10.3 Public Outreach

A utility may handle security and emergency response in a technically solid manner, but if the public is not properly informed, any situation can develop into a disaster. The public can be a utility's greatest ally in identifying and responding to a security breach, and proactive public outreach programs and policies can foster helpful activities.

Under normal conditions, public relations considerations can be necessary when performing day-to-day O&M. For example, the utility should seek community buy-in when security measures that will change the aesthetics of a facility are proposed. Gaining public acceptance before installing fencing and lighting in neighborhoods is critical.

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 Police Service (CHIPS) program case study. Using neighborhood awareness programs, such as infrastructure guards, can create a sense of awareness and, thus, confidence in utility operations, strategy, and agenda.

**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.

Informing citizens through a spokesperson who is trained in public or media communications is most effective. A Public Information Officer (PIO) is prepared to interact with local citizens and provide appropriate messages from the utility. The PIO may be a utility employee or a municipal employee, depending on the size of the utility. The PIO is selected before an emergency occurs and requires special public outreach training to be qualified to speak to the public and the media. 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. It is vital that the person designated to interface with the public and the media be trained to do so. Choose this person before an emergency occurs.

Some communities and police departments utilize a "reverse 911" system to notify customers of an emergency. This automatic dialing system enables several calls per minute to be made to citizens in a designated area. An informational recording can be played when the citizen answers the telephone.

Distributing information to the community quickly is an 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. Communication should be prompt, frequent, and reliable. A good article regarding public outreach concerns the Tylenol poisoning crisis from 1982.[15]

## 2.10.3 Communications Equipment

Many types of radios and telephones can be used to communicate with utility employees or with outside agencies such as the fire department:

- **Two-way radios** are a highly effective means of standard communication between dispatchers and field vehicles. Extra charged batteries should be carried at all times to prevent loss of contact. Note that the frequencies used by public utilities may not be compatible with emergency responder frequencies. Therefore, utilities are encouraged to have at least one radio that can communicate with first responders (typically 800 MHz). Training to use these 800 MHz radios is often available through police departments, fire departments, and local emergency managers. Utilities should understand that unsecured communications over two-way radios, including 800 MHz radios, may be intercepted and monitored by personnel other than those on the system. Also, utilities should learn from their local law enforcement agency and radio manufacturer whether to ban two-way radio communication in the vicinity of a bomb or possible bomb.
- **Cellular telephones** (cell phones) are becoming more popular, especially those with two-way radios built in. Again, extra batteries and/or a charger should be readily available. Cell phones, like two-way radios, should not be used during a bomb threat unless it is otherwise learned to be safe from local law enforcement and the radio manufacturer. It is important to remember that cell phone systems, as well as landlines, are frequently overloaded and may not be available for communications during disasters.
- **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.
- **Volunteer Amateur (Ham) Radio Operators** offer an alternate distance communication channel.

[15] "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).

If communications within the utility are disrupted or rendered useless in an event, the utility should contact its county or state Emergency Communications Coordinator (ECC) for assistance. The name and chain of command for the state and county ECCs should be maintained and current in the utility's Emergency Response Plan.

# 2.11 Interagency Coordination

An important part of protecting utility infrastructure involves interactions with other agencies. By reaching out to neighboring utilities, a wastewater utility may gain use of equipment and technical resources that it could not otherwise afford. Coordination with city or county offices such as emergency management agencies (e.g., Local Emergency Planning Committees [LEPCs]), health departments, law enforcement, and fire-rescue services may open doors for existing equipment, grants, and other assistance that the utility could not access or did not previously know existed. Coordination with other utility providers such as electric, gas, and telecommunications can also prove beneficial during an emergency.

## 2.11.1 Coordination with Other Wastewater Utilities

Not all inter-utility coordination should be performed locally because a large-scale disaster may render other wastewater systems in the vicinity unable to provide services or respond to other utilities' needs. Therefore, some coordination should be established with wastewater utilities located 80 kilometers (50 miles) or more away. It is recommended that, once utilities have come to an understanding about coordinating preparations and response in emergency situations, a mutual aid agreement be established to document the issues and avoid future misunderstandings. Further discussion regarding mutual aid agreements is presented in Section 2.11.3.

The following emergency measures should be considered when coordinating with other wastewater utilities:

- Interconnecting systems if possible and practical (with established rates and charges).
- Allowing treatment of wastewater at each other's facility if wastewater is brought in by tanker truck (with established rates and charges).
- Allowing solids processing at each other's facilities (with established rates and charges).
- Acquiring supplies and materials from another utility (with established rates and charges).
- Borrowing light and heavy equipment between utilities (with established rates and charges).
- Using staff from another utility (with established rates and charges).
- Holding periodic meetings (at least quarterly) to share information, renew contacts, update information, and review emergency response protocols.

## 2.11.2 Coordination with Other Agencies

To assure thorough emergency preparation and effective response, wastewater utility managers should develop relationships with a fairly broad spectrum of government agencies and other service providers, both locally and regionally. At the top of the list are law enforcement agencies, fire-rescue departments, and emergency management agencies. Ongoing coordination with other agencies, such as the local health department, public works department, water supply utility, and solid waste utility (to accept residuals should other disposal alternatives not be available), is also important, along with coordination with the wastewater utility's critical service providers, such as the electric utility, telecommunications utility and chemical suppliers. Wastewater utility managers should strive to see that the utility receives the highest level of reliability and responsiveness from its providers and suppliers.

Some action items to consider include:

- Invite local law enforcement and regional FBI personnel to a tour of the utility's facilities, including a briefing on system threats and vulnerabilities.
- Stress the importance of local law enforcement patrols past utility facilities and awareness of unauthorized access into collection systems or utility sites.
- Gain permission and learn to use emergency response radios and frequencies.
- Share telephone lists with key outside agencies.
- Provide a single point of contact for the utility during an emergency to all agencies that may be involved in a security problem or emergency response action.
- 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, providers, and suppliers to attend.
- Make sure that first responders are fully aware of all chemicals used and stored onsite so that proper equipment is available to safely and efficiently deal with explosions and/or fires.

## 2.11.3 Mutual Aid Agreements

Mutual aid agreements provide a formal means of documenting coordination efforts between utilities or other agencies and can greatly facilitate the exchange of resources during an emergency. They are based on the concept that resources, in most circumstances, are voluntarily provided, that there will be a reciprocal exchange if and when required, and that providing resources will not result in a profit to the providing party. While most wastewater utilities will enter into mutual aid agreements with other wastewater utilities, consideration should also be given to advantages that might be gained through mutual aid agreements with water, electric, and gas utilities as well.

Some of the benefits of entering into a mutual aid agreement with one or more utilities include the following:

- Commits the participating parties to a mutually beneficial, cooperative agreement based on principles and concepts of contract law, which support protecting public heath, the environment, and property.
- Provides a mechanism for coping with emergency situations that allows maximum flexibility in the use of resources.
- Reduces misunderstandings between parties, which often exist when assistance is requested or provided on an informal basis, especially during an emergency situation.
- Defines the parties involved; identifies respective responsibilities; and defines how and when they are to be implemented, who performs what and how, who pays for specific services, how long the agreement is in effect, how the agreements are terminated, and who administers the agreements.
- Provides for the utilization of resources to augment impacted or insufficient resources or capabilities of the other organization(s), thus allowing greater flexibility for all participants.
- Limits costs by overcoming budgetary restrictions, duplication of resources, equipment shortages, and operations or capabilities limitations.
- Provides that a party requesting assistance will indemnify the party providing the assistance for any resulting liability.
- Enhances communication and cooperation between the participating parties.
- Provides a legal basis for a participating party to operate outside its service area.

Mutual aid agreements may also specify that the parties providing assistance may withhold all or part of their resources under certain conditions.