Critical Infrastructure Protection

Water

Volume I:
Five Step Process to Define Threats, Develop & Implement the Security Plan

Don Philpott, Walter Presson Jr., and Cynthia Presson

Published by

Government Training Inc.™

ISBN: 978-1-937246-39-6

About the Publisher – Government Training Inc.™

Government Training Inc. provides worldwide training, publishing and consulting to government agencies and contractors that support government in areas of business and financial management, acquisition and contracting, physical and cyber security and grant writing. Our management team and instructors are seasoned executives with demonstrated experience in areas of federal, state, local and Department of Defense (DoD) needs and mandates.

For more information on the company, its publications and professional training, go to www.GovernmentTrainingInc.com.

This book has drawn heavily on the authoritative materials published by the a wide range of federal agencies including the Federal Emergency Management Agency (FEMA), the Department of Homeland Security (DHS), the Government Accountability Office (GAO), the General Services Administration (GSA), and the Headquarters, Department of the Army. These materials are in the public domain, but accreditation has been given both in the text and in the reference section, should you need additional information.

The authors and publisher have taken great care in the preparation of this handbook, but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or recommendations contained herein.

Government Training Inc. ™
Rights and Contracts Department
5372 Sandhamn Place
Longboat Key, Florida 34228
Don.dickson@GovernmentTrainingInc.com

ISBN: 978-1-937246-39-6

Government Training Inc.™

Physical Security & Grants

For more information on the company, its publications and professional training,
go to http://www.governmenttraininginc.com

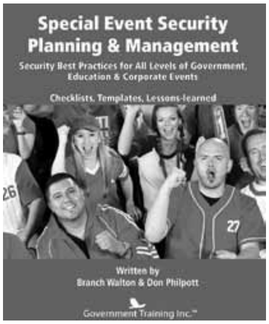
Guide to Physical Security Planning & Response
For Hospitals, Medical, & Long Term Care Facilities
Includes Comprehensive Section on Evacuation Best Practices
All-Hazards Planning & Response · Templates · Best Practices
Mary Russell, Jim Kendig, & Don Philpott
Government Training Inc.™

Guide to Physical Security Planning & Response

For Hospitals, Medical, & Long Term Care Facilities

This new—and timely—comprehensive guide is an A-to-Z of all-hazards planning for all healthcare facilities. While it is focused on hospitals, the guidance and procedures covered are equally relevant for nursing homes, assisted living facilities, and special needs homes.

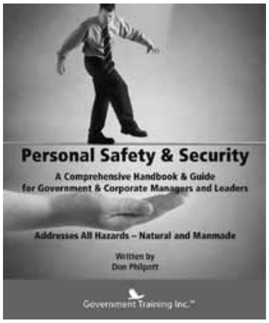
It is written by Florida experts who have enormous experience in emergency planning and evacuation having tackled major hurricanes and mass evacuations several times. Their expertise and lessons learned are documented throughout the book so that you can benefit from them.


Special Event Security Planning & Management
Security Best Practices for All Levels of Government, Education & Corporate Events
Checklists, Templates, Lessons-learned
Written by
Branch Walton & Don Philpott
Government Training Inc.™

Special Event Security Planning & Management

Security Best Practices for All Levels of Government, Education & Corporate Events

Don Philpott, a recognized international writer on security solutions, and Branch Walton, former U.S. Secret Service and corporate security advisor, have teamed-up to bring to the reader security best practices for events planning. The book draws on national and regional events lessons-learned and "right-sized" planning for all levels of government, education and corporate events. From local parades and public events to major sports and entertainment—all can use this practical guide.


Personal Safety & Security
A Comprehensive Handbook & Guide for Government & Corporate Managers and Leaders
Addresses All Hazards – Natural and Manmade
Written by
Don Philpott
Government Training Inc.™

Personal Safety & Security

A Comprehensive Handbook & Guide for Government & Corporate Managers and Leaders

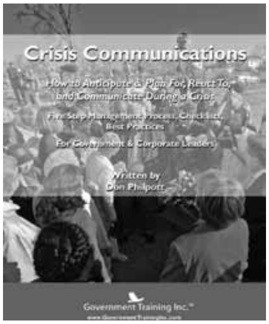
We all have a duty to our families, friends and loved ones to ensure that the places where we live, work, learn and play are secure, and that the people using them are safe.

The aim of this Handbook is not to alarm you, but to prepare and protect you. In the event of a disaster or terrorist incident, first responders may not be able to get to you immediately. Our goal is to give you the information you need so that you are aware of the various threats you face and how to recognize and respond to them.

Government Training Inc.™

Physical Security & Grants

For more information on the company, its publications and professional training,
go to http://www.governmenttraininginc.com

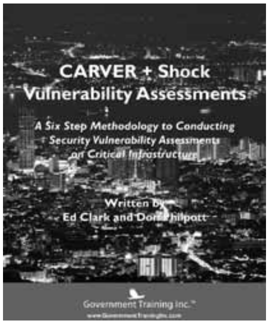

Crisis Communications
How to Anticipate & Plan For, React To, and Communicate During a Crisis
Five Step Management Process, Checklists, Best Practices
For Government & Corporate Leaders
Written by Don Philpott
Government Training Inc.™

Crisis Communications

How to Anticipate and Plan For, React To, and Communicate During a Crisis

Crisis planning and communications is an integral part of good management practice. By anticipating potential problem areas, identifying solutions, and being prepared you instantly remove a lot of the confusion and anxiety that arise when a crisis does occur.

If people know what to do, they can get on with performing their designated tasks immediately and, as a team, tackle the problem and get back to normal as quickly as possible.

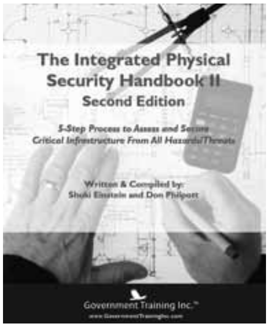

CARVER + Shock
Vulnerability Assessments
A Six Step Methodology to Conducting Security Vulnerability Assessments on Critical Infrastructure
Written by Ed Clark and Don Philpott
Government Training Inc.™

CARVER + Shock Vulnerability Assessment Tool

A 6-Step Approach to Conducting Security Vulnerability Assessments on Critical Infrastructuree

CARVER has served as the standard for security vulnerability assessments for many years. It has now morphed into an even more useful tool that can be used to help protect almost any critical infrastructure.

This new, no-nonsense handbook provides the security professional with background on CARVER, one of its very successful morphs into CARVER + Shock, and then demonstrates how these methodologies can be applied and adapted to meet today's specific needs to protect both hard and soft targets.


The Integrated Physical Security Handbook II
Second Edition
5-Step Process to Assess and Secure Critical Infrastructure From All Hazards Threats
Written & Compiled by: Shuki Einstein and Don Philpott
Government Training Inc.™

The Integrated Physical Security Handbook II 2nd Edition

5-Step Process to Assess and Secure Critical Infrastructure From All Hazards Threats

This new edition covers a number of additional areas including convergence of systems, building modeling, emergency procedures, privacy issues, cloud computing, shelters and safe areas, and disaster planning. There is also a comprehensive glossary as well as access to a dedicated website at **www.physicalsecurityhandbook.com** that provides purchasers of the book an online library of over 300 pages of additional reference materials.

Government Training Inc.™

Physical Security & Grants

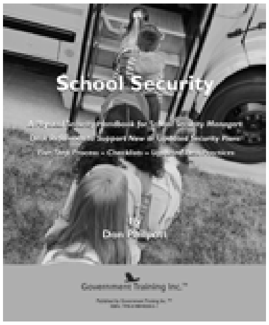
For more information on the company, its publications and professional training,
go to http://www.governmenttraininginc.com

Developing the Positive, Healthy & Safe Workplace
A 7-Step Management Process Leading to a Culture of Personnel Safety and Security
Guide for Government and Corporate Managers and Leaders
Written by
Rita Rizzo & Don Philpott
Government Training Inc.™

Developing the Positive, Healthy & Safe Workplace

A 7-Step Management Process Leading to a Culture of Personnel Safety & Security

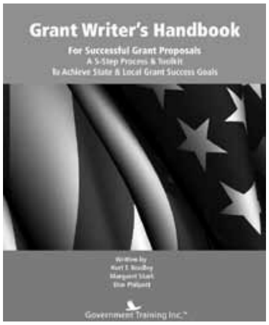
Rita Rizzo is a nationally recognized expert on all aspects of workplace quality, employee development, leadership and workplace security. Her thought-provoking seminars and books have brought practical solutions to the challenges of leadership. In the book, Rita presents a 7-step process for use by management and staff to create a positive, healthy, and safe workplace.



School Security

A Physical Security Handbook for School Security Managers

The School Security Handbook provides an easy to follow and implement 5-step process for developing an emergency response plan that covers almost any eventuality. It covers the phases of an emergency: mitigation and prevention, preparedness, response, and recovery.


Grant Writer's Handbook
For Successful Grant Proposals
A 5-Step Process & Toolkit
To Achieve State & Local Grant Success Goals
Written by
Don Philpott
Government Training Inc.™

Grant Writer's Handbook

A 5-Step Process & Toolkit to Achieve State & Local Grant Success Goals

The easy to follow 5-step process leads you through the tortuous world of grant writing—starting with how to select the right grant writer, and then following the process from where to find grants to writing winning grant submissions.

Contents

Photographs in this book provided by FEMA, www.fema.gov

Symbols

Throughout this book you will see a number of icons displayed. The icons are there to help you as you work through the Six Step process. Each icon acts as an advisory – for instance alerting you to things that you must always do or should never do. The icons used are:

❗ This is something that you must always do

⊘ This is something you should never do

💡 Really useful tips

⚑ Points to bear in mind

☑ Have you checked off or answered everything on this list?

About the Authors

Don Philpott

Don Philpott is editor of International Homeland Security, a quarterly journal for homeland security professionals, and has been writing, reporting and broadcasting on international events, trouble spots and major news stories for more than 40 years. For 20 years he was a senior correspondent with Press Association -Reuters, the wire service, and traveled the world on assignments including Northern Ireland, Lebanon, Israel, South Africa and Asia.

He writes for magazines and newspapers in the United States and Europe and is a contributor to radio and television programs on security and other issues. He is the author of more than 130 books on a wide range of subjects and has had more than 5,000 articles printed in publications around the world. His most recent books are The Integrated Physical Security Handbook II, Crisis Communications, Special Event Security, Planning & Management, and Personal Safety & Security. All of these books have been published by Government Training Inc.

He is a member of the National Press Club.

Walter "Butch" Presson Jr.

Walter "Butch" Presson Jr. has been employed at the SC Environmental Training Center at Central Carolina Technical College since 1995, enhancing the credibility of the ETC as the premier water and wastewater training provider in South Carolina. His reputation as an effective, knowledgeable instructor and water professional is known throughout the state with over 40 years of experience in the water/wastewater industry.

Butch holds South Carolina A-level operator licenses in Water Treatment, Biological Wastewater, Physical/ Chemical Wastewater and a B-level license in Water Distribution. He was the Water Environment of South Carolina's (WEASC) Swamp Fox District and Association Wastewater Operator of the Year in 1982, and was the first Chair of the WEASC Swamp Fox District in 1980. He served on the Water Environment Association Board of Directors (1986-87) and currently serves on the SC Environmental Certification Board's Continuing Education Committee. He is a member of the American Water Works Association, Water Environment Association of South Carolina and the Water Environment Federation.

Cynthia Presson

Cynthia Presson, Executive Director of the SC Section of American Water Works Association and the Water Environment Association of South Carolina, has been working in the environmental field for more than 20 years.

With a BS degree in Agronomy from LSU and a Masters in Business Management with emphasis on Non-Profit Leadership from New England College, Cindy has worked in various environmental areas during her career, including genetic, tissue culture and disease research on small fruit plants, wet chemistry lab analyses, hazardous waste treatment, storage, disposal and transportation, water & wastewater treatment & operations, environmental training & development, and association management. She holds SC A-level operator licenses in Physical/Chemical & Biological Wastewater treatment and a B-level in Water Treatment. Cindy is a Certified Environmental Trainer, including water/wastewater operations and facility vulnerability assessment and security.

Acknowledgements

This manual has drawn heavily upon the authoritative materials published by the Federal Emergency Management Agency (FEMA), Department of Homeland Security (DHS), Government Accountability Office (GAO), General Services Administration (GSA), Environmental Protection Agency (EPA) and many other state and federal agencies. These materials are in the public domain and accreditation has been given both in the text and in the reference section. In some instances, when official reports are being mentioned in this book, opinions are stated. These are the opinions of expert witnesses and members of the report's panel, not the opinions of the authors. They are included, however, because they do contribute to the debate on protecting the nation's water infrastructure.

This book is based on the unique five step process developed for the Integrated Physical Security Handbook (Government Training, Inc.) for protecting the nation's critical infrastructure.

Introduction

In general, the threat of drinking water contamination through terrorist activities is small. To be effective, most contaminants would need to be used in very large quantities, thereby minimizing an actual threat, and treatment processes already in place will deactivate many contaminants. Also, following 9/11, drinking water utilities across the nation were alerted about the need to increase security and have augmented surveillance and protection measures.

The primary threats to the Nation's drinking water supplies are contamination by chemical, biological or radiological agents; damage, destruction, or sabotage of physical infrastructure; and disruption to computer systems. Generally, biological agents considered to be weapons of mass destruction pose the most danger in aerosol form (i.e. direct exposure to pathogens transported in the air).

There are also threats from natural disasters such as hurricanes, earthquakes and floods. All of these issues have to be taken into account when developing an effecting emergency response plan that must cover every eventuality.

The water sector consists of two basic components: potable water supplies and wastewater collection and treatment. According to EPA there are approximately 53,000 community water systems in the United States. EPA's data reflects that ownership of these systems is evenly split—about half are publicly owned by state and local authorities and about half are privately owned.

According to EPA, the majority of the U.S. population gets its water from publicly owned systems.

Community water systems vary by size and other factors but most typically include a supply source, such as surface water or groundwater, a treatment facility, which uses (and stores) chemicals such as chlorinealum, lime, etc. to eliminate pathogens and reduce taste and odor problems, and a distribution system which includes water storage towers, piping grids, valves, pumps, and other components necessary to deliver treated potable water to consumers. Community water systems often contain many miles of pipe with numerous access points that may be vulnerable to terrorist attack.

The USA PATRIOT Act defines critical infrastructure as those "systems and assets . . . so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

The National Strategy for Homeland Security grouped the critical infrastructure of the United States into 13 sectors—agriculture, banking and finance, chemical, defense industrial base, emergency services, energy, food, government, information and telecommunications, postal and shipping, public health, transportation, and water sectors.

Remember

These systems are often taken for granted because they are so basic to our daily lives that we only notice them when our service is disrupted.

President Bush designated a lead agency for each of the 13 sectors to coordinate interaction between the federal government and the private sectors. The lead agency for the chemical sector is the Department of Homeland Security (DHS) and the lead agency for the water sector is the Environmental Protection Agency (EPA).

There are about 15,000 critical facilities—including chemical, water, energy, and other sector s—that produce, use, or store more than threshold amounts of chemicals the EPA has estimated pose the greatest risk to human health and the environment. Of these 15,000 facilities, DHS estimates there are about 4,000 chemical manufacturing facilities. There are approximately 53,000 community drinking water systems and more than 2,900 maritime facilities that are required to comply with certain provisions of the Maritime Transportation Security Act of 2002 (MTSA).

In addition, there are approximately 77,000 dams and reservoirs, thousands of miles of pipes, aqueducts, water distribution and sewer lines, 168,000 public drinking water facilities and about 16,000 publicly owned wastewater treatment facilities (POTWs). The federal government has ownership responsibility for hundreds of dams and diversion structures, but the vast majority of the nation's water infrastructure is either privately or publicly owned by non-federal units of government.

Terrorist attacks upon our nation's infrastructure could have a significant impact on the health and safety of millions of Americans and result in environmental damage and/or economic disruption.

The public and private sectors are working diligently to secure critical assets in chemical, water, and maritime facilities, but much more is necessary to guarantee the safety and security of the nation's critical water infrastructure.

□ In the United States, water utilities treat nearly 34 billion gallons of water every day.

□ In the United States and Canada, there are approximately one million miles of water pipeline and aqueducts - enough to encircle the globe 40 times.

□ Americans consume more than one billion glasses of tap water per day

□ From birth to 6 months, children consume seven times as much water per pound as the average American adult.

The following five step process was developed by Shuki Einstein and myself for our *Integrated Physical Security Handbook.*

In order to carry out a comprehensive assessment of facility necessities, an understanding of the basic elements of security is required- what you are protecting and how vulnerable it is. Knowledge and understanding of threat sources and mitigation and principles of deterrence, detection, delay, response, recovery and re-evaluation is critical, along with all available options Armed with this knowledge you can develop and implement the most appropriate integrated physical security plan for your facility.

When planning, there are two scenarios – if and when. The "if" scenario covers planning and procedures to prevent the likelihood of an incident. The "when" scenario covers planning and response procedures after an incident and is mainly concerned with mitigation and recovery.

Remember that the cost to mitigate and recover may be less than the cost to protect so there must always be a balance between protection and mitigation and an analysis of both.

Step One – Your Model Secure Facility

Now that you have an understanding of basic security techniques and applications relating to facility protection, at the next step is consideration of a model secure facility – the facility that in a perfect world is able to maximize security without compromising business as usual. Many methodologies omit this step, but we believe it is important to examine what would constitute a model secure facility for you; one which has identified its core functions, critical assets, threats and vulnerabilities and taken the appropriate measures to mitigate them. Above all, it is a facility that is secure yet one that is able to carry on its core function efficiently and effectively. Once you have identified your model facility, you have a benchmark for comparison.

Step Two - Gap Analysis: How do you compare with the model facility?

The goal of physical security is to protect facilities and the assets contained therein. The most important of these assets is, of course, the people. Items to be identified initially include:

- assets to be protected.
- threats to those assets.
- vulnerability of those assets
- priorities

> Fact: 85% of all critical infrastructures and key resources in the U.S. are privately-owned.

What Am I Protecting?

Protective systems should be developed for specific assets. Assets are anything key to your mission that can be destroyed, damaged or stolen. The risk-analysis procedure is used to identify assets –from the building itself to hazardous materials, equipment, supplies, furniture, computers, IT infrastructure and, of course, people.

Identification of core functions will enable you to identify the specific critical infrastructure to be protected in order to maintain operations in the event of an attack.

Differing layers of security may be necessary in various parts of the facility based upon the value of the assets located there. For instance, there should be relatively free access to the kitchen/lunch room but much greater restricted access to the computer network control room.

Asset value is determined by considering the following three elements:

- criticality of the asset
- ease of replacement.
- measure of relative value.

Who Are My Adversaries?

It is important to identify and characterize both internal and external threats to these assets either from within or without the facility. Internal threats include pilfering of office equipment, theft of classified information or disgruntled employees who may sabotage equipment, disrupt operations, or physically harm other employees. External threats range from break-ins, vandalism and theft to acts of terrorism. It is important to understand your adversaries' tactics, motivations and capabilities. Consult your local police, the FBI and other agencies that monitor identified and potential threats. They can advise on possible threats, their source, and what methods and weapons may be utilized.

Other resources include:

- **Design Base Threat (DBT)** – analysis to help identify likely adversaries, their strengths and capabilities, potential targets and the likelihood and method of attack.
- **Crime Prevention Through Environmental Design (CPTED)** – a tried and trusted methodology which takes into account the relationship between the physical environment its users. It is a useful tool in identifying potential crimes and their perpetrators.

Where Am I Vulnerable?

A useful method of identifying threats is to conduct scenario- based assessments. This is an extremely analytical process that employs the identification of critical flaws and weak points in your current physical protection through the development of multiple "what if" scenarios. By working through various scenarios and determining probable actions and consequences, you can then develop plans to counter or mitigate them.

Must Do

Until you discover your areas of vulnerability, you cannot develop strategies to protect them.

Use the model facility as your benchmark to identify areas of your facility that need attention. Conduct an audit of your facility – site boundaries, building construction, room locations, access points, operating conditions (working hours, off-hours, etc.), existing physical protection features, safety considerations and types and numbers of employees and visitors.

Next, determine all critical assets, tangible and intangible- equipment, personnel and materials. This analysis should also include facility /employer reputation, employee morale and proprietary information.

You must identify and characterize vulnerabilities that would allow potential threats to be realized. A major problem for buildings in urban areas is lack of a secure perimeter,. enabling a vehicle containing a bomb to approach within several feet of a building, causing major damage upon detonation. Internal vulnerabilities include poorly trained security staff and lack of access controls to sensitive parts of the building.

Include an assessment of the impact of an incident at a nearby facility—a chemical spill for instance—and necessary steps to protect your property and people.

By identifying weaknesses you can develop solutions to reduce or eliminate them.

What Are My Priorities?

Risk assessment must take into account the impact on your business or operation if assets are destroyed or damaged. Part of that assessment is to rate the impact of the loss as low, medium or high. This will identify critical assets requiring maximum protection.

How do I compare?

Once you have established critical assets, potential threats, areas of vulnerability and protection priorities, you are in a position to perform a Gap Analysis to identify steps to reduce risk, increase safety and provide necessary physical security for your facility by comparison to the model facility..

Step Three - Gap Closure

Having identified your deficiencies, you must then consider and evaluate all available options to mitigate the threats. There is a vast array of systems and devices available and you must determine the best options for your particular circumstances and budget. If you have questions about products and services, it is best to consult an independent security consultant rather than a vendor with a vested interested in sales.

General options are described as follows:

1) Perimeter Security

Securing the perimeter, stopping or delaying entry, surveillance and detection, protection basics, defense measures, standoff distances and responses to reduce security risks.

2) Vehicles

Protecting approaches, controlling access and parking, installing barriers, surveillance and other monitoring equipment.

3) Internal Security

Access controls, alarms and barriers, authentication devices and screening, access biometrics, CCTV, hot site protection, safe mail rooms, coping with hazards, etc..

4) Information Technology

Integrating IT, cyber and physical security planning, providing network/infrastructure protection and protecting files, document and other critical resources.

5) Personnel

- **Security Staff** - requirements/hiring/screening/training, security programs and responses
- **Staff/visitors** - screening/training/informing; drills/evacuation/safe rooms; alarms/staging areas; communications and coping with and recovering from an event.
- **Special needs** - ADA requirements and special resources.

6) Building Design/Security

Building codes, exits/fences/gates/doors/barriers; windows, critical floor space/safe rooms/safe areas; devices/detectors; lighting, cameras and maintenance.

7) Community Risk Assessment/ Involvement

Assessing local risks and incorporating into planning; working with fire/police/EMS, local businesses and residents.

8) Technology Solutions

The handbook deals with the various security and defense devices available to you. These are referred to in Security 101 and the Gap Analysis and Gap Closure chapters in general terms. References are provided throughout the book for more comprehensive information should you need it.

Step Four - Strategic Plan

Having identified assets, adversaries, threats & vulnerabilities and determined priorities and options, you are in a position to plan and strategize the security change process. This means developing a road map; plotting how to get where you want to be from where you are. The strategic plan sets out Steps Two and Three above – documenting your Gap Analysis, identifying critical assets, threats and weaknesses and all areas needing to be addressed. The Gap Closure documents how you plan to close those gaps, the justification for the actions to be taken, costs involved and timeframe for implementation.

Remember

The strategic plan serves two critical functions: it is the marketing tool you need to get management approval and it is the blueprint for your physical security plan.

Step Five - Implementation

Once your Strategic Plan has been approved, it must be implemented. This includes project management, bid contracting and vendor selection, quality assurance and quality control and revising policy procedures.

Integrated physical security planning is an ongoing requirement. Once your system is in place you must continuously test it for weaknesses and vulnerabilities and ensure that your employees understand why the measures are in place and their roles in the event of an emergency.

Re-analyze – what is my current situation? Ask yourself what has changed and what new threats have emerged since your last review By regularly tracking and monitoring your integrated physical security system you can close gaps and introduce enhancements.

The following section may be used as a general reference in establishing a safe, secure facility.

10 Key Features of an Active and Effective Security program

1. Integrate protective concepts into organizational culture, leadership, and daily operations. Foster attentiveness to protection in the day-to-day thinking of front-line workers, emergency responders, management, and senior leadership. Identify employees responsible for implementing security priorities.

2. Identify and support security program priorities, resources, and utility-specific measures. Dedicate resources to specific protection needs through annual capital, operations and maintenance budgets, and/or staff resource plans. Develop measures appropriate to utility-specific circumstances and operating conditions

3. Employ protocols for detection of contamination. Establish working relationships with local, state, and public health communities to detect public health anomalies and evaluate them for contamination implications. Track, characterize, and analyze customer complaints to identify potential contamination events.

4. Assess risks and review vulnerability assessments (VAs) .Maintain current understanding and assessment of threats, vulnerabilities, and consequences. Establish and implement a schedule for review of threats, vulnerabilities, and consequences and their impact on the vulnerability assessment at least every 2-3 years to account for factors such as facility expansion/upgrades, community growth and advancing technology.

5. Establish facility and information access control. Implement physical and procedural controls to restrict utility access to authorized personnel only. Define, identify, and restrict access to security-sensitive information (both electronic and hard copy) for utility operations and technical details.

6. Incorporate resiliency concepts into physical infrastructure. Include security program considerations early in the design, planning, and budgeting processes to mitigate vulnerability and/or potential consequences and improve resiliency. Develop design and construction specifications that address both physical hardening of sensitive infrastructure and adoption of inherently lower risk technologies and approaches where feasible.

7. Prepare, test, and update emergency response and business continuity plans. Understand, train personnel, and implement National Incident Management System (NIMS) guidelines and Incident Command Systems (ICS). Review and update emergency plans annually and test those plans through tabletop, functional, and full-scale exercises.

8. Develop partnerships with first responders, managers of critical interdependent infrastructure, other utilities, and ancillary response organizations. Forge partnerships in advance of an emergency, ensuring utilities and key partners are better prepared to work together if an incident should occur. Establish relationships with critical customers (hospitals, manufacturing, first responders, etc.) to identify interdependency issues that may impact business continuity and utilize state Water/Wastewater agency Response Network (WARN) systems where available.

9. Develop and implement internal and external communication strategies. Motivate staff to support security program strategies and goals. Prepare key messages for various types of emergencies and determine how those messages should be delivered to the community and by whom.

10. Monitor local, regional, national and global incidents and threat-level information. Develop systems to access threat information, identify threat levels, and determine specific response actions (e.g., WaterISAC).