Security & Preparedness in the Water Sector

June 9, 2010

Bath, Michigan
Overview

— Key Drivers
  – Legislation
  – Presidential Directives

— AWWA & Sector Initiatives
  – Standards & Guidance
  – Mutual Aid & Assistance
  – Emergency Water Supply
  – Contamination Warning Systems
  – Cyber/Process Control Systems
Security & Preparedness Drivers

- Bioterrorism Act
- Patriot Act
- Homeland Security Act
- Critical Infrastructure Information Protection Act
- Intelligence Reform Act
- Homeland Security Presidential Directives (HSPDs)
Homeland Security Presidential Directives

— HSPD-5: Management of Domestic Incidents
  • National Incident Management System (NIMS)
  • National Response Plan (NRP)
— HSPD-7: Critical Infrastructure Identification, Prioritization and Protection (replaces PDD-63)
  • National Infrastructure Protection Plan (NIPP)
  • Sector Specific Plans (SSP)
— HSPD-8: National Preparedness
— HSPD-9: Defense of Ag & Food
— HSPD-10: Biodefense for the 21st Century
— HSPD-12: Common Identification Standard
— HSPD-20: National Continuity Policy
The Water Sector Vision

A secure and resilient drinking water and wastewater infrastructure that provides clean and safe water as an integral part of daily life. This Vision assures the economic vitality of and public confidence in the nation's drinking water and wastewater through a layered defense of effective preparedness and security practices in the sector.
SSP Goals

1. Sustain protection of public health and the environment.
2. Recognize and reduce risks in the water sector.
3. Maintain a resilient infrastructure.
4. Increase communication, outreach, and public confidence.
4. Selecting Disinfectants in a Security-Conscious Environment
Purpose: This standard defines the minimum requirements for a protective security program for a water or wastewater utility that will promote the protection of employee safety, public health, public safety, and public confidence.

This standard builds on the long-standing practice amongst utilities of utilizing a multiple barrier approach for the protection of public health and safety.
Requirements:

a) Explicit Commitment to Security
b) Security Culture
c) Defined Security Roles and Employee Expectations
d) Up-To-Date Assessment of Risk (Vulnerability)
e) Resources Dedicated to Security and Security Implementation Priorities
f) Access Control and Intrusion Detection
g) Contamination, Detection, Monitoring and Surveillance
h) Information Protection and Continuity
i) Design and Construction
j) Threat Level-Based Protocols
k) Emergency Response and Recovery Plans and Business Continuity Plan
l) Internal and External Communications
m) Partnerships
n) Verification
1) Asset Characterization
What assets do I have that are critical to my operations?

2) Threat Characterization
What reasonable worst case threat, natural hazard & supply chain scenarios should I consider?

3) Consequence Analysis
What happens to my assets & operations if attacked by terrorists, natural hazards or supply chain disruption? How much money lost, to me? fatalities? injuries? How much economic loss to the Community?

4) Vulnerability Analysis
What vulnerabilities would allow a terrorist, natural disaster or supply chain problems to cause these consequences? Given the scenario, what is the likelihood it will result in these consequences?

5) Threat Assessment
What is the likelihood that a terrorist natural disaster or supply chain disruption will strike my operations?

6) Risk / Resilience Assessment
Risk = Consequences \times (Vulnerability \times Threat)
Resilience = Service Outage \times (Vulnerability \times Threat)

7) Risk / Resilience Management
What options do I have to reduce risks & increase resilience and continuity? How much will each benefit my organization? How much will it cost? What is benefit/cost ratio of my options? How can I manage the chosen options?
**Purpose:** This standard defines the minimum requirements for emergency preparedness for a water or wastewater utility. Emergency preparedness practices include the development of an emergency response plan (hazard evaluation, hazard mitigation, response planning, and mutual aid agreements), the evaluation of the emergency response plan through exercises, and the revision of the emergency response plan after exercises.
Selecting Disinfectants in a Security Conscious Environment

- Provide guidance to water, wastewater, and reuse utilities
- Framework to evaluate disinfection alternatives that:
  - Reflects local circumstances
  - Addresses utility’s specific disinfection objectives
  - Provides framework to compare options consistently and transparently
  - Accounts for reliability, safety, and other key criteria
  - Reflects the need to incorporate risk communication within process
  - Scaleable across system sizes
  - Integrates risk-based performance measures for security based on CFATS
Resiliency Initiatives

— Mutual Aid & Assistance
  – WARN
  – Resource Typing
— Emergency Water Supply
  – National Strategic Plan
  – Healthcare
— Contamination Warning Systems
— Cyber/Process Control Systems
The WARN Action Plan
(March 2006)

- WARN Agreement
  - Voluntary
  - No Obligation
  - No cost
  - Liability/Workmans Comp
  - Reimbursement process
  - Element of NIMS
  - All-Hazards
Emergency Water Supply

— National Strategic Plan for Emergency Water Supply
  — EPA-NHSRC/AWWA collaboration
  — Provide guidance for utility preparedness
  — Develop recommendations to clarify roles and responsibilities under current or new ESF

— Emergency Water Supply Planning for Hospitals and Health Care Facilities
  — CDC/AWWA collaboration
  — Address gaps in Joint Commission standards
The Contamination Scenario

— What is the objective of a contamination warning system?
— What are the appropriate monitoring technologies?
— Where do we put the monitors and how often do we monitor?
— How do we integrate and analyze the indicator data?
— What would constitute an alarm?
— What do we do when the alarm goes off?
Cyber Security

Vision

In 10 years, industrial control systems for critical applications will be designed, installed, and maintained to operate with no loss of critical function during and after a cyber event.

Key Strategies

- Develop and Deploy ICS Security Programs
- Assess Risk
- Develop and Implement Protective Measures
- Partnership and Outreach
Additional Resources