Infrastructure Security for Public Water and Wastewater Utilities

Presented by
Joe Burns
Kentucky Rural Water Association

July 19, 2005
Public Health Security and Bioterrorism Preparedness and Response Act of 2002

Drinking Water Safety and Security
Requirements

• Vulnerability Assessments
  – >100,000 population by March 31, 2003
  – 50,000 – 100,000 by December 31, 2003
  – 3,300 – 50,000 by June 30, 2004

• Emergency response plans
  – within 6 months of vulnerability assessment

• USDA additional requirements
  – All borrowers both water and wastewater must complete VA and ERP no matter population
What is a Vulnerability Assessment

• Evaluate a utility to determine what threats (terrorist, vandal, etc) they may be susceptible to
• Identify corrective actions that can reduce or mitigate the threats.
• Provides a guide to utility that prioritizes upgrades and procedural policy changes
Common Elements of Vulnerability Assessments

1. Characterization of the water system, including its mission and objectives;
2. Identification and prioritization of adverse consequences to avoid;
3. Determination of critical assets that might be subject to malevolent acts that could result in undesired consequences;
4. Assessment of the likelihood (qualitative probability) of such malevolent acts from adversaries;
5. Evaluation of existing countermeasures; and
6. Analysis of current risk and development of a prioritized plan for risk reduction.
What is the Reality of a Breach?

- What scenarios or events could compromise a utility?
- Are they possible?
- What is the likelihood?
The “SEMS” VA Process

- Contact Info
- Mission/Threat
- All Assets
- Critical Customers
- 45 Questions
- Add’l protection
- Prioritized Report
What is the Mission of my Utility?

• Mission of the utility
  – Safe potable water?
  – Fire protection?
  – Protection of public health?
  – Protection of the environment
  – Others?

• Is one mission more important than the other
  – Fire protection vs. safe water
  – Rural vs. city

• Increase in mission (or threats) invariably increase costs.

Step 1:
Mission
How could an attack take place?

• Threats
  – Vandal
  – Disgruntled employee
  – Terrorist
  – Other

• For assistance:
  – Evaluate history of community
  – Contact local law enforcement, FBI, DHS
  – U.S. EPA “Baseline Threat Information” document

Step 4:
  Threats
What are the Critical Assets in my System?

• Identify all assets of utility
• Other concerns
  – Redundancy – spare pumps, parts, pipe
  – Back up power - Generator
  – Geographic importance
  – Critical customers (hospitals, govt buildings, etc)
  – Highest area or percentage of customers

Step 3: Critical Assets
What are common critical assets at Water Utilities?

Typical single points of failure:

- Intake pumps
- Pumping stations
- Well pumps and motors
- Treatment facilities
- Chlorinator
- Chemical feeds
- Piping and distribution system
- Clear wells (ground water storage)
- Elevated storage (water towers)
- Power supply
- Others

Step 2:
What to Avoid
What are common critical assets at Wastewater Utilities?

Typical single points of failure:

- Lift stations
- Manholes
- Collection system
- Treatment facilities
- Chlorinator
- Chemical feeds
- Power supply
- Others

Step 2:
What to Avoid
So, is Everything Critical?

- Can’t protect against everything – What will take you out the quickest?
- What is the easiest target to hit?
- What are my most critical customers? – Govt, military, industry, densely populated?
- Think about
  – How long would you be down?
  – How widespread would the impact be?
  – How severe?

Step 2:
What to Avoid
What are the most effective protective measures based on threat?

- Based on the threat, identify single points that if attacked would impact mission, critical customers, or disrupt service to many customers -
  - For example
    - Could not serve water to 70% of community
    - Could not provide adequate water for fire fighting
    - Power plant would not be functional
    - Contaminate streams or public health

- **Countermeasures needed – 45 questions**

  Step 4: Threats
What protection do I currently have?

- Existing detect, delay, respond
- Existing cyber protection
- Existing security policies and procedures

Steps 4 and 5 are done simultaneously in SEMS

Step 5:
Existing Security
How Should I Prioritize?

- Local decision based on threats, location, size, resources, local information, etc.
- For example – With limited resources
  - Pump station responsible for serving few of the total community, customers located in rural area, and no critical customers – Finding: LOW priority
  - PWS name not displayed on vehicle - Finding MED priority
  - No neighborhood watch program – Finding: HIGH priority
  - No controlled use of hydrants – Finding: HIGH priority
  - Critical facilities unlocked – Finding: HIGH priority

Step 6:
Prioritization
What can I do to protect my System?

- Reduce DETECTION time – policies and procedures, alarms, video, lighting
- Increase DELAY time – barriers, locks, fences, security guards, neighborhood watch
- Reduce RESPONSE Time – planning, coordination, and training

Step 6: Prioritization
DETECTION

- Access Control – Card keys, punch codes,
- Manual – CCTV, check ID’s
- Alarms
- Motion detectors
- High tech intrusions sensors
- Inspect deliveries
- Landscape maintenance
- Lighting
- Raw and finished wastewater monitoring
DELAY

• Barriers
  – Jersey barriers
  – Vehicle tires
  – 55 gallon barrels
• Fences
  – Chain link
  – Barbed or Razor wire
• Locks – gates, fences, doors, windows, hatches, fill pipes
• Harden doors and hinges
RESPONSE

• Public warning system
• Flow gates to divert contaminants
• Use alternative to gaseous chlorine
• Coordination with local first responders
• Emergency response plan
• PRACTICE and TRAINING!
Results
Common Security Enhancements Systems < 10,000

- Employee awareness and training
- Fencing
- Locks
- More patrols
- More signs
- Neighborhood watch
- Intrusion alarms
- More lighting
Questions?