Michigan Water Utility Security Summit; Water System Resilience

June 7, 2011 – Bath, MI

AWWA National Update

Copyright © 2011 American Water Works Association
Objectives

• What is security? resilience?
• Homeland Security Drivers
• Role of Standards & Guidance
• What is in the future for water security?
Security and Resilience

Guns/Gates/Guards vs Response, Recovery, Resilience
Key Points in Time

- December 7, 1941 – Pearl Harbor
- April 19, 1995 – Oklahoma City
- December 31, 1999 – Y2K
- September 11, 2001 – WTC, Pentagon, PA
- August 29, 2005 – Katrina
- April/May 2011 – Extensive Tornado activity and Flooding in Midwest and Southeast
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.
# Standards & Guidance

**AWWA Security & Preparedness Resources**

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Manuals</td>
<td>M10: Emergency Planning for Water &amp; Wastewater Utilities [revision pending]</td>
</tr>
<tr>
<td>Manuals</td>
<td>J100: RAMACAP Risk &amp; Resilience</td>
</tr>
<tr>
<td>Manuals</td>
<td>Utilities Helping Utilities Action Plan (WARN Model)</td>
</tr>
<tr>
<td>Manuals</td>
<td>Training Resources</td>
</tr>
<tr>
<td>Manuals</td>
<td>Resources Typing Manual</td>
</tr>
<tr>
<td>Manuals</td>
<td>BCP Guidance [under development]</td>
</tr>
<tr>
<td>Manuals</td>
<td>B300 Site</td>
</tr>
<tr>
<td>Manuals</td>
<td>?? Potential ??</td>
</tr>
</tbody>
</table>

## Training Resources
- Emergency Response Planning, 2003
- Security Hardware, 2004
- Contamination Monitoring Technologies, 2003
- Cyber Security, 2003
- Crisis Communication Seminar, 2004
- First Responder Training, 2006
Standards & Guidance

3. Water Infrastructure Security Enhancements (WISE)
5. M19: Emergency Planning for Water Utilities
Origins of the G430 Standard

- Post 9/11, Minimal Guidance and Direction
- Early Efforts Focused Only on Specific Pieces
  - WISE focused on physical security
- EPA’s National Drinking Water Advisory Council (NDWAC) Forms the Water Security Working Group in 2004
  - 14 Features of an Active and Effective Security Program Presented in June 2005
  - Moving from Just Terrorism to All Hazards
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
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
Where is Management?
Hopefully this is not the answer
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
Brief History of RAMCAP

9/02: ASME-White House-industry infrastructure workshop recommends consistent risk management methods comparable across sectors

4/04: Professional societies, National Labs, DHS & other Federal Agencies review RAMCAP; advise: “KEEP IT SIMPLE”

1/06: First five Sector-Specific Guidance documents are completed

6/06: DHS issues NIPP, designates RAMCAP as the key critical infrastructure protection methodology

9/07: Work completed on Dams & Water Sectors and Regional Resilience conceptual design

1/08: RAMCAP Campus method & software developed

8/08: RAMCAP Plus® -- all hazards, dependencies, dual economics, benefit-cost analysis

1/09: ASME-ITI and AWWA establish a joint standards committee to develop J100

1/10: ASME-ITI and AWWA Boards approve J100 Standard

5/10: ANSI approval; J100 is first RAMCAP standard issued
RAMCAP’s Consistency and Comparability

- A uniform risk/resilience analysis methodology that provides
  - Common terminology
  - Common metrics
  - Common process
  - Common scenarios
  - Consistent results

Necessary for the comparability essential to resource allocation

- The RAMCAP process is not intended to be the most comprehensive and detailed risk assessment methodology – but it is intended to be
  - Practical and efficient to apply,
  - Cumulative over time, and
  - Effective in enhancing security and resilience
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 regional 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 Likelihood Analysis

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

6) Risk / Resilience Likelihood

Risk = Consequences x (Vulnerability x Threat Likelihood)

Resilience = Service Outage x (Vulnerability x Threat Likelihood)

7) Risk / Resilience Management

What options do I have to reduce risks, increase resilience and value? How much will each benefit my organization? My region? How much will it cost? What is benefit/cost ratio of my options? How can I manage the chosen options?
The RAMCAP Plus Process Is Selective

1) Asset Characterization
2) Threat Characterization
3) Consequence Analysis
4) Vulnerability Analysis
5) Threat Likelihood Analysis
6) Risk / Resilience Analysis
7) Risk / Resilience Management

Non-Critical & Low-Consequence Facilities
Non-Critical Assets in Critical Facilities
Low-Consequence Critical Assets in Critical Facilities
Low-Consequence Threat-Asset Pairs
Low-Consequence Threat-Asset Pairs
Threat-Asset Pairs w/ Acceptable Risk/Resil.
Low Net Benefit Options

STOP: Defer or Eliminate
J100 Includes the Utility Resilience Index (URI)

Utility Resilience Index = ORI + FRI

Where:

ORI = Operational Resilience Index, comprised of seven equally weighted indicators

FRI = Financial Resilience Index, comprised of five equally weighted indicators
Operational Resilience Sub-index Indicators

1. Emergency Response Plan
2. National Infrastructure Management Plan Compliance
3. Mutual aid & assistance agreements
4. Emergency power for critical operations
5. Ability to meet minimum daily demand (water) or treatment (wastewater) when the plant is non-functional
6. Critical parts & equipment
7. Critical staff resilience
Financial Resilience Sub-Index Indicators

1. Business Continuity Plan
2. Utility Bond Rating
3. Governmental Accounting Standards Board: Statement #34 Assessment (GASB 34)
4. Unemployment
5. Median Household Income
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
Water Infrastructure Security Enhancements (WISE)

- Water Infrastructure Security Enhancements (WISE)
  - EPA supported collaboration between ASCE/AWWA/WEF
  - Purpose is to provide basic security design guidance manuals for the water and wastewater sector that offer practical and appropriate solutions on the following:
    - Guidelines for the Physical Security of Water Utilities
    - Guidelines for the Physical Security of Wastewater/Stormwater Utilities
    - Guidelines for Designing an Online Contaminant Monitoring System
- Released in 2007.
- www.awwa.org/science/wise/
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
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?
ANSI/AWWA G430-09:
Security Practices for Operations and Management

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
Cyber Threats are Real

- Director of National Intelligence confirms control systems are being targeted for exploitation (2008)
- Remotely modified Sacramento River control (2007) < former employee? >
- Malware Infection at Harrisburg Water System (2006) < overseas hacker >
- Catastrophic Failure at Taum Sauk Water Storage Dam (2005) < instrumentation / accident >
- Sewage Spill at Maroochy Shire (2000) < disgruntled job applicant >
How to deal with Cyber Threat?

• SSP Goals clarified need to develop strategy to address key questions
  
  • How would our operations change if we did not have SCADA working?
  
  • How sure are we that our SCADA systems are secure?
  
  • When was the last time we performed cyber security vulnerability assessments?
  
  • What would be the impact to our organizations if we were aware of vulnerabilities and did nothing?
Roadmap Development

Purpose: Develop a shared vision and strategy for improving the cyber security of water systems

- September 20, 2007
- San Jose, CA
- 30 participants from 23 organizations across the U.S.

- Future Trends
- Vision for Securing Control Systems
- Goals and Milestones
- Key Challenges
- Next Steps
Vision & Strategies to Secure Control Systems

**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
Process Control System Resources

- USCERT – [www.us-cert.gov](http://www.us-cert.gov)

- Cyber Security Evaluation Tool (CSET) a systematic and repeatable approach for assessing the cybersecurity posture of their industrial control system networks…. contact [cset@dhs.gov](mailto:cset@dhs.gov).

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

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.
M19: Emergency Planning for Water Utilities

- Core Elements:
  - Hazard Summary
  - Vulnerability Assessment
  - Mitigation Actions
  - Preparedness Planning
  - Emergency Response, Recovery & Training

- Complements G430, J100, G450
Resiliency Initiatives

- Mutual Aid & Assistance
- Emergency Water Supply
- Business Continuity Planning
Water\Wastewater Agency Response Network (WARN)

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

www.NationalWARN.org
March 2011 (48)
Successful Uses of WARN

- CalWARN
  - Northridge Earthquake, 1994
  - El Nino Storms, 1998
  - Sonora Fires, 2001
  - Southern California Fires, 2007
  - Baja Earthquake, 2010

- FlaWARN
  - Hurricanes Katrina, Wilma and Rita, 2005
  - Tornadoes, 2007

- OrWARN
  - Detroit, Blizzard 2008

- TxWARN
  - Rain Storms and Hurricane Humberto, 2007
  - Hurricane Dolly and Ike, 2008

- CoWARN
  - City of Alamosa Salmonella outbreak, 2008

- TNWARN, INWARN, KYWARN
  - Ice Storm February 2009
City of Alamosa Salmonella outbreak, March – April, 2008

• Major effort was to:
  – Determine the source of contamination
  – Inform the public
  – Establish a logistical system for the distribution of clean water
  – Remove the contamination from the system

• CoWARN response consisted of:
  • 23 water and wastewater utilities working together, including the Colorado Rural Water Association
  • State of Nebraska (through the Mid-America Alliance)

• Large and small CoWARN members worked together to provide:
  • Technical expertise, equipment, and supplies
  • Critical system disinfection and water sampling support
Emergency Timeline & Mutual Aid

WARN does not require state or federal declaration and includes public and private drinking water and wastewater utilities.

- **Alamosa Salmonella Outbreak**
- **CDPHE Notified 3/19/08**
- **CoWARN Activated 3/19/08**
- **Gov. Ritter declares state of emergency in Alamosa on 3/21/08**
- **Order lifted 4/11/08**
Success and Opportunity

• Major Incidents with Intrastate WARN activation

• Major Lessons Learned
  ▪ Roles/Responsibilities
  ▪ Communications and Power
  ▪ Self-sufficiency
  ▪ Interstate issues need resolution
Emergency Water Supply

- National Strategic Plan for Emergency Water Supply
  - EPA-NHSRC/AWWA collaboration
  - Provide guidance for utility preparedness
  - Clarify roles and responsibilities

- Emergency Water Supply Planning for Hospitals and Health Care Facilities
  - CDC/AWWA collaboration
  - Address gaps in Joint Commission standards
What is a BCP?

• A plan for how your utility will stay continuously in business during and after various forms of disasters impacting your utility.
  • How will you communicate internally and externally?
  • How will you pay your employees and how will you collect your revenue?
Objective

• To provide water utilities with an understanding of the nature, triggers and components of business continuity planning, and how a Business Continuity Plan (BCP) is different from but complementary to an Emergency Response Plan (ERP) and Disaster Recovery Plan (DRP).
• To provide a sample business case, including cost-benefit analysis, as to why BCPs are important to utilities and how they fit into the organizational structure.
• Using case studies, to provide water utilities with an understanding of how business continuity plans have been developed and implemented in water utilities, and how they have performed.
• To provide water utilities with an overview of different levels of investment in BCPs, and guidance such as decision support tools (including a size-sensitive template, and a business case template) for utilities to select the approach that will work best for their circumstances.
• To provide training materials that can be used by water utilities as a basis for developing and implementing a BCP.
BCP Plan Umbrella

HAZARD MIITIGATION PLANS

Spill Prevention Control & Countermeasures (SPCC)

Safety Plans

Business Continuity Plan (BCP)

Continuity of Operations Plan (COOP)

Emergency Operations Plan (EOP) / Emergency Response Plan (ERP)

Continuity of Government (COG)

Risk Management Plan (RMP)

Vulnerability Assessment (VA)

Hazard Assessment (HA)

Threat Assessment (TA)

Business Risk Assessment

HAZARD IDENTIFICATION & ASSESSMENTS

HAZARD-SPECIFIC PLANS

Pan Flu Plan
Natural Hazard Plans
Power Outage Plan
Contamination Plan
Drought / Conservation / Curtailment Plan
All Hazards Plan
Others

SPECIALIZED SUPPORTING PLANS

Finance/Administrative Plan
Crisis Communications Plan (CCP)
Disaster Recovery Plan (DRP) IT
Security Plan
Mutual Aid Plans
Event Recovery Plan
Mitigation Plan
What is happening with Chemical Security?
Objectives

• What is state of chemical security in water sector, specifically chlorine?

• What is in the future for chemical security in the water sector?
Chemical Facility Anti-Terrorism Standards (CFATS)

1. Appendix A – list of chemicals and thresholds used by DHS to conduct a rough screen and prioritize sites
   - Over 40,000 sites to be evaluated
   - Assess for theft/diversion, sabotage, offsite consequence and economic criticality

2. Sites preliminarily deemed high risk must complete a vulnerability assessment – Chemical Security Assessment Tool for tiers 1 – 3 and other approved methods for tier 4.

3. 19 Risk-Based Performance Standards will apply in whole or in part based upon vulnerabilities identified in step 2 above – sites select the appropriate combination based upon case-by-case analysis
   - DHS guidance is being prepared to explain each metric in detail

4. DHS reviews and approves site specific plans – which codify the performance metrics and CSAT results – once approved the site implements the measures

5. Enforcement includes $25,000 fines and potential facility shutdown for non-compliance
Scope of Current Regulation

- 40,000+ Potentially High-Risk Chemical Facilities
- 300+ sites

Tiers:
- I
- II
- III – 1,000+
- IV – 6,000+

Low Risk – 32,000+

* ALL Drinking Water & Wastewater systems are exempt and not required to take any action under CFATS at this time
CFATS Risk-Based Performance Standards

DHS rule components for “high risk sites” –

- 18 performance measures are identified including:

<table>
<thead>
<tr>
<th>Restrict Area Perimeter</th>
<th>Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Site Assets</td>
<td>Training</td>
</tr>
<tr>
<td>Screen and Control Access</td>
<td>Personnel Surety</td>
</tr>
<tr>
<td>Detect, Deter and Delay</td>
<td>Elevated Threats</td>
</tr>
<tr>
<td>Shipping, Receipt and Storage</td>
<td>Specific Threats</td>
</tr>
<tr>
<td>Theft and Diversion</td>
<td>Reporting Incidents</td>
</tr>
<tr>
<td>Sabotage</td>
<td>Significant event response</td>
</tr>
<tr>
<td>Cyber Security</td>
<td>Designating Officials</td>
</tr>
<tr>
<td>Response</td>
<td>Recordkeeping</td>
</tr>
</tbody>
</table>
Chlorine Gas Use and Supply Type

- No Chlorine Gas: 595, 40.8%
- Use Chlorine Gas: 863, 59.2%

Bar chart showing responses:
- 150lb cylinder: 51.3%
- 1 ton container: 63.1%
- Tanker: 2.9%
- Rail: 3.2%
## Potential Water Sector CFATS Triggers

<table>
<thead>
<tr>
<th>Chemical of Interest</th>
<th>Release (lbs)</th>
<th>Theft (lbs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ammonia (anhydrous)</td>
<td>10,000</td>
<td></td>
</tr>
<tr>
<td>Chlorine (gaseous)</td>
<td>2,500</td>
<td>500</td>
</tr>
<tr>
<td>Chlorine dioxide</td>
<td>1,000</td>
<td></td>
</tr>
<tr>
<td>Hydrochloric acid</td>
<td>15,000</td>
<td></td>
</tr>
<tr>
<td>Hydrochloric acid (≥ 37% conc.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hydrogen peroxide</td>
<td></td>
<td>400</td>
</tr>
<tr>
<td>Hydrogen peroxide (≥ 35% conc.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hydrogen chloride (anhydrous)</td>
<td>5,000</td>
<td>500</td>
</tr>
<tr>
<td>Potassium permangante</td>
<td></td>
<td>400</td>
</tr>
</tbody>
</table>
Selecting Disinfectants in a Security Conscious Environment

- Recognize that drinking water treatment is not simple
- Treatment decisions are heavily constrained
  - SDWA regulations,
  - Production demands, and
  - Customer affordability.
- Changes to water treatment must be thoughtful
  - Consider the effects those changes will have on the quality of water provided to consumers,
  - Evaluate the sustainability of the treatment process over time and under adverse conditions
- Evaluation must be transparent
  - Assure technically sound for the system’s own use
  - Facilitate adequate regulatory review
  - Open to public scrutiny
Guide Overview

• 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
Water systems are making disinfectant changes, today

- SDWA regulatory compliance
  - Stage 1 Disinfectants and Disinfection Byproducts Rule
  - Ground Water Rule
  - Stage 2 Disinfectants and Disinfection Byproducts Rule
  - Long-Term 2 Enhanced Surface Water Treatment Rule

- Security concerns
  - Vulnerability assessments
  - Post-Katrina awareness of the importance of all-hazards preparedness and system resiliency

- Responding to local concerns
  - Disinfection goals
  - Community safety
Key Points for Drinking Water Utilities

• Regulations lead to multiple disinfection barriers
• Several viable disinfection alternatives exist
  • free chlorine,
  • chloramines,
  • chlorine dioxide,
  • ozone,
  • UV, and
  • combinations.
• Each alternative has applications for different purposes… no “one size fits all”
• U.S. regulatory paradigm will continue to require the use of chlorine at WTPs for the foreseeable future
Disinfection Evaluation and Selection Process

• Reflects a stepwise process
• Consistent with engineering practice
• Fair to all disinfectant options
• Incorporates risk communication throughout
Implementation

• Prioritize disinfection project(s) relative to other water system improvements
  • Asset management
• Design and communication of change
  • Regulatory review
  • Re-evaluate planning assumptions if necessary
• Schedule construction
  • External milestones
  • Integration with other projects
• Maintain risk communication effort
  • Adapt communication to construction phase
Selecting Disinfectant Guide

- Distributed electronically free of charge to AWWA’s utility members
- Available for purchase from AWWA bookstore
- Copies distributed to SDWA primacy agencies through ASDWA
- Integrated into AWWA standard and guidance development efforts
CFATS Legislative Outlook

• House
  • HR 901 - extend by 7 years; no provisions for inherently safer technologies (IST) or civil suits.
  • HR 908 – similar to HR 901, but managed by E&C vs. Homeland…jurisdiction issues

• Senate
  • S 473 – 3 yr extension, no IST, includes voluntary training and technical assistance
  • S 711 – Secure Water Facilities Act…includes IST mandate, representation in VA development, civil suits allowed
Additional Resources
Questions

Kevin M. Morley
Security & Preparedness Program Manager
AWWA – Government Affairs
1300 Eye Street, NW Suite 701W
Washington, DC 2005
202-628-8303 or kmorley@awwa.org

Advancing Security and Emergency Preparedness in the Water Sector