Conducting Water Sector Risk and Resilience Assessments: A WaterISAC Webinar Series

Webinar #1

August 27, 2019
WaterISAC Mission

Protect Utilities

Information sharing
Background

- Established in 2002 at the urging of the White House, FBI and US EPA
- Created by the water and wastewater sector
- Focused solely on the sector’s security needs
- Dues-based non-profit
Areas of Focus

• Physical Security
  – Terrorism
  – Other malicious activity
• Cybersecurity
  – Business/Enterprise System
  – Industrial Control System
• Natural Disasters
• Other Hazards
Information Gathering, Curation, Analysis & Dissemination

Federal
DHS, FBI, US EPA, State Dept, FEMA, CDC, NOAA, others

State/Local
Law Enforcement, Homeland Security, Fusion Centers

Cross-Sector
Other ISACS, Other Critical Infrastructure Sectors

Other
Subject Matter Experts, Security Firms, Research Orgs, Utilities, Media

Threats Analyses | Threat Alerts
Mitigation Resources
Best Practices | Webinars
Weekly Updates

Members
Membership

• Water and wastewater utilities
• Consulting and engineering firms
• Local, state and federal agencies

• Dues: tiered based on size and organization type
• 60-day free trial membership
• Join at waterisac.org
Housekeeping

• The webinar is being recorded.

• The recording and slide deck available tomorrow at waterisac.org/webcasts.

• Q&A at the end.
How to Ask a Question

Raise your hand

- or -

Type and send
Presenters

• John McLaughlin, PE
  Merrick & Company
CONDUCTING WATER SECTOR RISK AND RESILIENCE ASSESSMENTS

A WaterISAC Webinar Series
Webinar #1 – August 27, 2019
INTRODUCTION

• Civil engineer w/ 40 years experience
• Organized a Disaster Response effort after hurricane Floyd, 1998
• Original NC AWWA-WEA Disaster Preparedness committee 2002, now Risk Management committee
• Joint ASCE / AWWA / WEF Water Infrastructure Security Enhancements guidance committee, 2002-05
• GAO water security funding priority study, 2002
• AWWA G430 standard committee, Present
• AWWA M-19 committee, Present
• Original AWWA J100-10 standard committee, 2008 - 2010
• Chair AWWA J100-10 standard update committee, 2018 to present
• Led more than forty VA’s / RA’s
WHAT THIS IS, WHAT WE WILL COVER

- Background & History
- Vulnerability Assessment vs. Risk and Resilience
- Requirements of the America’s Water Infrastructure Act of 2018 (AWIA)
- Risk and Resilience Process Following AWWA J100-13
- To Get You Thinking: Critical Asset Examples
- Summary
BACKGROUND & HISTORY
PRE 9/11
SECURITY

• Primarily natural disasters
• “Security” concerns dominated by natural events
• Emergency response focused on natural events
• Intentional acts largely considered unconnected and unreported
• November 1941 - J. Edgar Hoover in AWWA Journal – water systems are critical and vulnerable

Utility impacts after Hurricane Floyd
POST 9/11
TERRORISM

• Required to complete Vulnerability Assessments using RAM-W™, VSAT™ e.g.
• Focused on a terrorist attack at a utility, physical security
• Given only 6-months to “complete” an Emergency Response Plan sets the tone. Focused on terrorism.
• No All Hazards approach
• No Risk and Resilience Management
CURRENT TIME (~2004 to PRESENT)

ALL HAZARDS

• AWWA J100-13 standard is adopted (2010, update 2013)
• Utilities began focusing on a holistic or all hazards approach
• Still struggling to see the importance of utility risk and resilience management
  • Not a terrorist target
  • Many more priorities
  • Not required
• J100 reinforced the all hazards approach at the national level
• Uses a dollar value of risk in decision making
• Cause and Effect way of approaching risk
• America’s Water Infrastructure Act of 2018 (AWIA) signed into law
• See the following all hazards examples....
Present Day Condition Based Failure

1998 NE & Canada Ice Storm

2018 Hurricane Florence

2011 Alabama Tornadoes
VULNERABILITY ASSESSMENT VS. RISK AND RESILIENCE (SECURITY)
VULNERABILITY ASSESSMENTS TO RISK AND RESILIENCE ASSESSMENTS

<table>
<thead>
<tr>
<th>VULNERABILITY ASSESSMENTS</th>
<th>RISK AND RESILIENCE ASSESSMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Focus primarily on Vulnerabilities</td>
<td>Looks at Risk and Resilience</td>
</tr>
<tr>
<td>Qualitative values for Consequence</td>
<td>Dollar values for Consequence</td>
</tr>
<tr>
<td>Threat Likelihood = Low, Medium or High, or 1.0</td>
<td>Actual Probability of occurrence used for Threat Likelihood</td>
</tr>
<tr>
<td>Multiple approaches, no standard</td>
<td>Development of one, water sector specific standard (J100)</td>
</tr>
<tr>
<td>Qualitative output was Low, Medium, High not in dollars</td>
<td>Output in dollars (benefit-cost)</td>
</tr>
</tbody>
</table>
REQUIREMENTS OF AMERICA’S WATER INFRASTRUCTURE ACT (AWIA)
“EACH COMMUNITY WATER SYSTEM SHALL CONDUCT AN ASSESSMENT OF THE RISKS TO, AND RESILIENCE OF, ITS SYSTEMS.”

- Malevolent acts and natural hazards
- Resilience of
  - Pipes and constructed conveyances
  - Physical barriers
  - Source water, water collection & intake
  - Pretreatment & treatment
  - Storage & distribution facilities
  - Electronic, computer, or other automated systems
- Monitoring practices
- Financial infrastructure
- Use, storage, or handling of various chemicals
- Operation and maintenance
- May include an evaluation of capital and operational needs for risk and resilience management
EPA’s August 1st Required Information, Including Baseline Threat Information

- Certification Deadlines
- Risk and Resilience Assessment Requirements and Assistance Resources
- Emergency Response Plan Requirements and Assistance Resources
- Certification Process
- Third-Party Standards
- Final Disposition of Bioterrorism Act Vulnerability Assessments
- Training
- Fact Sheet
- Five-year Review, Revision and Certification Requirements
### KEY DIFFERENCES BETWEEN 2002 BIOTERRORISM ACT AND 2018 AWIA

<table>
<thead>
<tr>
<th>2002 BIOTERRORISM ACT</th>
<th></th>
<th>2018 AWIA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Assessment</td>
<td>Risk &amp; Resilience Assessment</td>
<td></td>
</tr>
<tr>
<td>Terrorism focus</td>
<td>All hazards</td>
<td></td>
</tr>
<tr>
<td>Submittal required</td>
<td>Certification only</td>
<td></td>
</tr>
<tr>
<td>Develop an ERP</td>
<td>Prepare/update ERP &amp; Certify</td>
<td></td>
</tr>
<tr>
<td>Cyber not mentioned</td>
<td>“Electronic, computer, or other automated systems” included*</td>
<td></td>
</tr>
<tr>
<td>Non compliance - Federal offense</td>
<td>Non compliance - Federal offense</td>
<td></td>
</tr>
</tbody>
</table>

* - See the WaterISAC’s Cyber Assessment webinar series
THE RISK AND RESILIENCE PROCESS FOLLOWING AWWA J100-13

OVERVIEW
SEVEN STEPS OF J100-13

1. Asset Characterization

2. Threat Characterization
   • Intentional, Natural, Dependency, Proximity
   • Select relevant threats from the J100 reference threat library or see also EPA Baseline Threat guidance

3. Consequence Analysis
   • Fatalities, Injuries, Utility Economic Loss, Regional Economic Loss

4. Vulnerability Analysis
   • Relative to Threat-Asset pairs. Think like the threat, layers.

5. Threat Analysis
   • What is the likelihood that the threats selected in step 2 will act upon on the assets selected in step 1?
     • The Proxy method for terrorist acts
     • See also EPA Baseline Threat guidance

6. Risk/Resilience Analysis
   • What is the existing level of risk/resilience?
     • Risk = Consequence x Vulnerability x Threat
     • Resilience = (Outage Duration x Outage Severity) x Vulnerability x Threat

7. Risk/Resilience Management
   • Options to reduce risk/increase resilience, cost-benefit

Details for each step in Webinars 2 and 3
SOME EXAMPLES OF CRITICAL ASSETS

• This is your homework, think about this
• Single points of failure, wherever they are
• Categories out of AWIA to assess
  • Physical barriers,
  • Source water,
  • Pipes, constructed conveyances, water collection, intake,
  • Pretreatment and treatment,
  • Storage and distribution,
  • Electronic, computer or other automated systems,
  • Monitoring practices,
  • Financial infrastructure,
  • Use, storage handling of chemicals,
  • O&M of utility
SOME EXAMPLES OF CRITICAL ASSETS

• Homework (cont.)

• Some typical, specific critical assets
  • Electrical switchgear, is this centralized?
  • Unmonitored CCTV/Access control
  • Single raw water source, inadequate interconnects
  • Reliance on SCADA systems, could you operate manually?
  • Key plant staff, succession planning, brain drain, pandemic
  • Generators and fuel supplies, are they adequate?
  • Chemical supplies and feed equipment
SUMMARY,
WHAT TO REMEMBER

- Risk and Resilience Management is good operational practice
- Creates efficiency through prioritization, risk management
- It’s measurable
- It’s the law now
- AWWA J100-13 is the industry standard for risk and resilience
- Reduced Risk + Increased Resilience = Security
- Webinars 2 & 3 – The J100 process in greater detail

John W. McLaughlin, PE
Merrick & Company
704-996-6895
john.mclaughlin@merrick.com
How to Ask a Question

Raise your hand

- or -

Type and send
Upcoming Risk and Resilience Assessment Webinars

• September 11 - Step-by-step walk through of the process of performing a J100-based assessment

• October 2, 2019 - Final steps of a J100-13 based assessment, plus some examples of typical risk and resilience management strategies and options

• Register at waterisac.org/events.
Upcoming Cyber Assessment Webinar

• September 18 - Focus on the IT or business systems identified in AWIA. How the OT and IT components of the assessment will work together to meet the risk and resiliency assessment requirements for AWIA.

• Register at waterisac.org/events.
Other Resources

waterisac.org/awia

Links to helpful resource by EPA, AWWA and other partners.
Thank You

Contact

John W. McLaughlin, PE
john.mclaughlin@merrick.com
704-996-6895

Michael Arceneaux
Managing Director
arceneaux@waterisac.org

Mikko McFeely
Resilience Program Manager
mcfeely@waterisac.org

1-866-H2O-ISAC