Emergency Operations Plans and Cybersecurity Considerations

Steve Vance and Dave McMillan.

Illinois Rural Water Association

A Review

- America's Water Infrastructure Act (AWIA) – Section 2013
  - Water systems serving more than 3,300 people must develop or update risk assessments and emergency response plans (ERPs).
  - Must re-certify the RRA and ERP every five years – You are certifying that you have reviewed and amended as needed

Illinois Requirement

Section 604.135 Repair Work and Emergency Operation

d) Emergency Operations Plan

1) Each community water supply must develop an emergency operations plan for the provision of water under emergency circumstances, including earthquakes, floods, tornados, and other disasters. The emergency operations plan **must include a review of the methods and means by which alternative supplies of drinking water could be provided in the event of destruction, impairment or contamination of community water supply.**

2) The community water supply must **review its emergency operations plan at least every three years and revise the plan as necessary.** must maintain the emergency operations plan on site and make it available to the Agency, upon request.

Additional Emergency Planning Measures

Section 604.155 Electrical Controls and Standby Power

a) Electrical controls must be located above grade, in areas not subject to flooding.

b) Each community water supply must provide on site, dedicated **standby power** capable of maintaining continued operation of its water system during power outages to meet the average daily usage determined under Section 604.115.

Section 604.160 Safety

a) All community water supplies whose treatment involves chemical application must have and maintain a **chemical safety plan**.

b) All community water supply personnel involved in the use and maintenance of chemicals must have **periodic safety training**.

Risk and Resilience Assessment Requirements

Six required elements:

- **Risk to the system** from malevolent acts and natural hazards;
- **Resilience** of the pipes and constructed conveyances, physical barriers, source water, water collection and intake, pretreatment, treatment, storage and distribution facilities, electronic, computer, or other automated systems (including the security of such systems) which are utilized by the system;

Six required elements continued:

- The **monitoring practices** of the system;
- The **financial infrastructure** of the system;
- The use, storage, or handling of **various chemicals by the system**; and
- the **operation and maintenance** of the system.

Emergency Response Plan Requirements

Four elements:

- **Strategies and resources to improve the resilience of the system**, including the physical security and cybersecurity of the system;
- **Plans and procedures that can be implemented, and identification of equipment that can be utilized,** in the event of a malevolent act or natural hazard that threatens the ability of the community water system to deliver safe drinking water;

Four elements continued:

- **Actions, procedures and equipment which can obviate or significantly lessen the impact** of a malevolent act or natural hazard on the public health and the safety and supply of drinking water provided to communities and individuals, including the development of alternative source water options, relocation of water intakes and construction of flood protection barriers; and
- **Strategies that can be used to aid in the detection** of malevolent acts or natural hazards that threaten the security or resilience of the system.

Coordination with local emergency

- Community water systems shall to the extent possible coordinate with local emergency planning committees established under the Emergency Planning and Community Right-To-Know Act of 1986 when preparing or revising an assessment or emergency response plan under the AWIA.
- Further, systems must maintain a copy of the assessment and emergency response plan for five years after certifying the plan to the EPA.

RRA/ERP/EOP ARE ALL CONFIDENTIAL

- RRA/ERP YOU ONLY CERTIFY COMPLETION – DON'T SEND THE ASSESSMENT OR PLAN TO ANYONE
- EOP WILL BE EVALUATED DURING YOUR INSPECTION
  - IF YOU GET DINGED FOR INCOMPLETE OR LACK OF A PLAN, DO NOT SEND IN YOUR PLAN, CERTIFY THAT YOU HAVE COMPLETED IT IN YOUR RESPONSE LETTER AND INDICATE IT IS AVAILABLE FOR ON-SITE REVIEW

Tools and Methods

https://www.epa.gov/waterresilience

U.S. EPA **recommends** using AWWA J100-10 Risk and Resilience Management of Water and Wastewater Systems along with other tools from U.S. EA and other organizations.

AWIA **does not require** the use of any standards, methods or tools for the risk and resilience assessment or emergency response plan.

Environmental Topics | Laws & Regulations | About EPA

Drinking Water and Wastewater Resilience

CONTACT US

SHARE

Register for Risk Assessment and Emergency Response Plan Webinar

EXIT

Register for In-person Risk Assessment and Emergency Response Plan Training

Not sure where to start?

Download the 2018 Route to Resilience.

Not sure where to start?
Download the 2018 Route to Resilience.

Assess

- Conduct a risk assessment
- Learn financial and health impacts of a water disruption
- Creating Resilient Water Utilities
- Adopt cybersecurity best practices

Plan

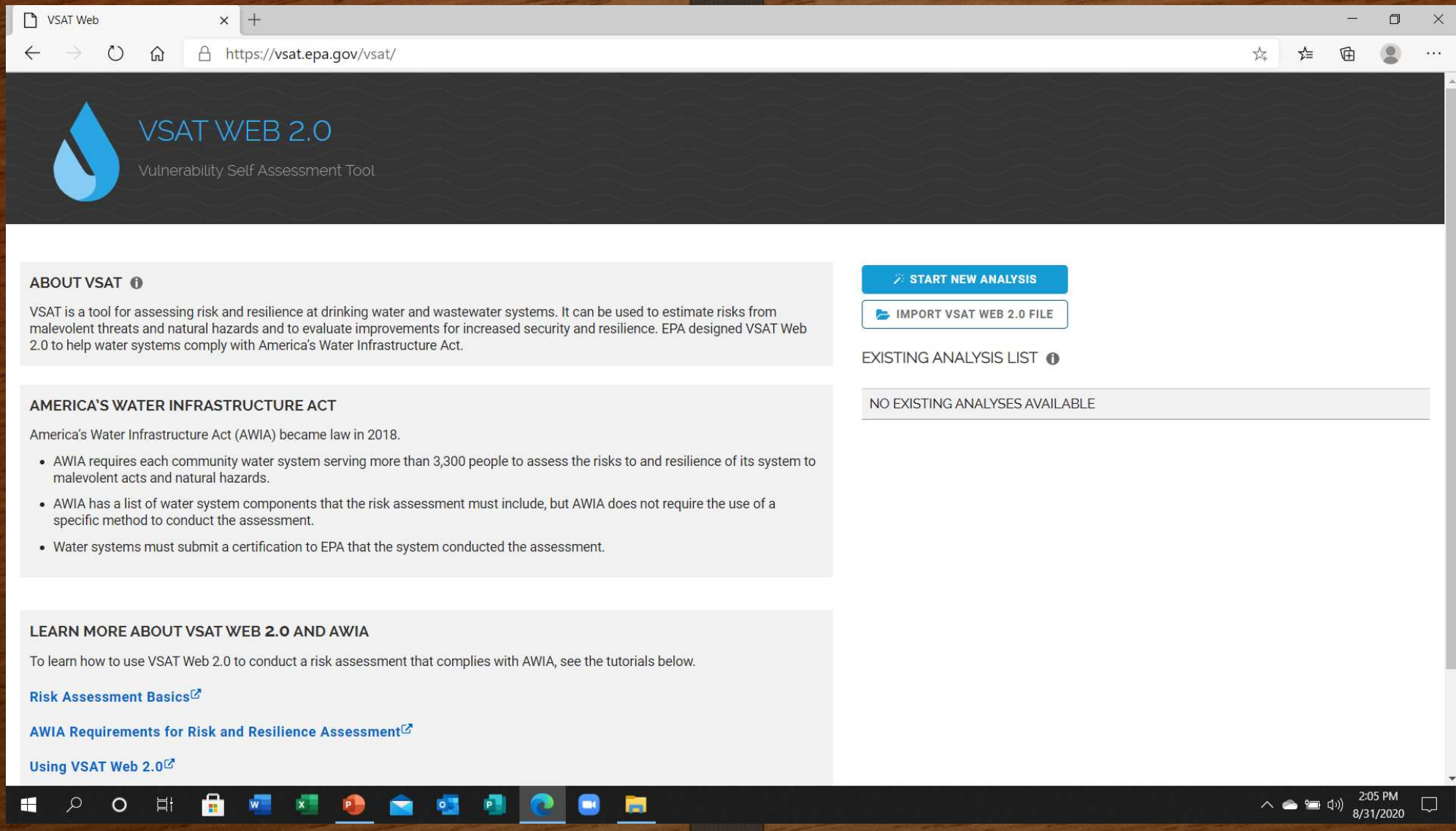
- Develop emergency response plans
- Build hazard resilience
- Build relationships in your community
- Share resources during an emergency

Learn About Water Resilience

- Water resilience basics
- Protect your local water supply
- Technical support products and services

Join Our Email List

Related Sites


VSAT Web
https://vsat.epa.gov/vsat/
VSAT WEB 2.0
Vulnerability Self Assessment Tool
ABOUT VSAT
VSAT is a tool for assessing risk and resilience at drinking water and wastewater systems. It can be used to estimate risks from malevolent threats and natural hazards and to evaluate improvements for increased security and resilience. EPA designed VSAT Web 2.0 to help water systems comply with America's Water Infrastructure Act.
AMERICA'S WATER INFRASTRUCTURE ACT
America's Water Infrastructure Act (AWIA) became law in 2018.
AWIA requires each community water system serving more than 3,300 people to assess the risks to and resilience of its system to malevolent acts and natural hazards.
AWIA has a list of water system components that the risk assessment must include, but AWIA does not require the use of a specific method to conduct the assessment.
Water systems must submit a certification to EPA that the system conducted the assessment.
LEARN MORE ABOUT VSAT WEB 2.0 AND AWIA
To learn how to use VSAT Web 2.0 to conduct a risk assessment that complies with AWIA, see the tutorials below.
Risk Assessment Basics
AWIA Requirements for Risk and Resilience Assessment
Using VSAT Web 2.0
START NEW ANALYSIS
IMPORT VSAT WEB 2.0 FILE
EXISTING ANALYSIS LIST
NO EXISTING ANALYSES AVAILABLE
2:05 PM
8/31/2020

45 Page Document- 5 Chapters – Chapter 2 – 8 Elements of an ERP

II. Emergency Response Plan—Eight Core Elements
A. System Specific Information (Element 1)

B. CWS Roles and Responsibilities (Element 2)

C. Communication Procedures: Who, What, and When (Element 3)

1. Internal Notification List
2. 2. External Non-CWS Notification List
3. Public/Media Notification: When and How to Communicate

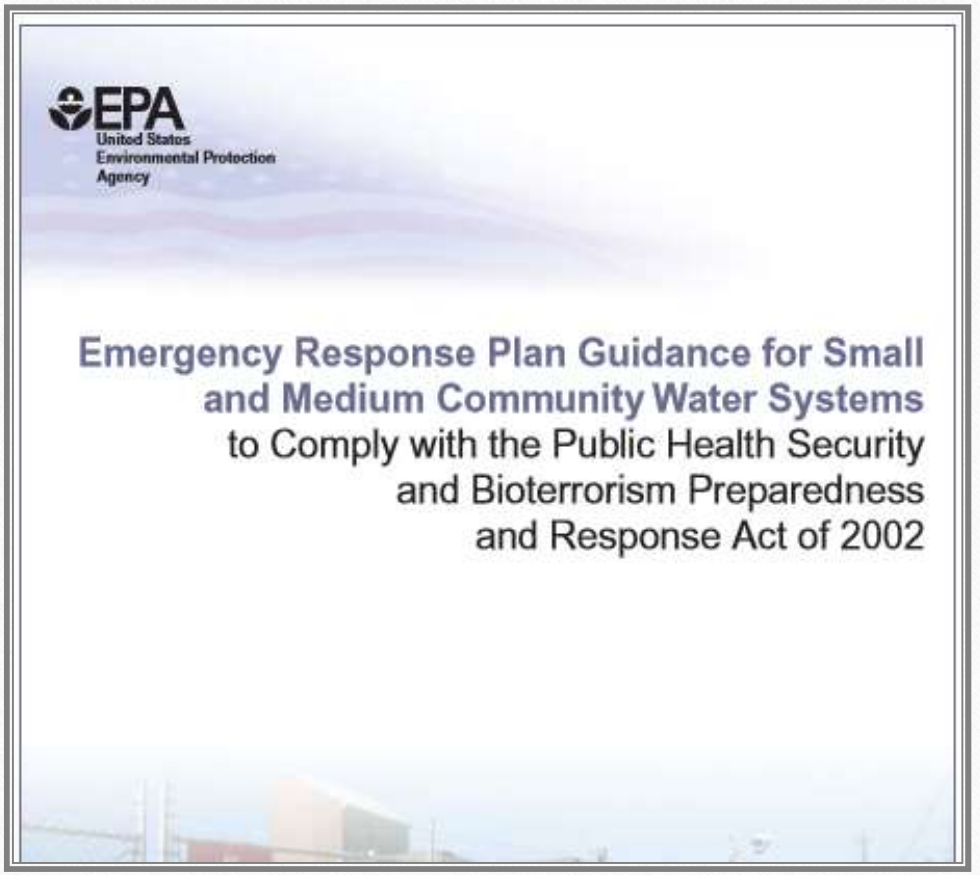
D. Personnel Safety (Element 4)

E. Identification of Alternate Water Sources (Element 5)

F. Replacement Equipment and Chemical Supplies (Element 6)

G. Property Protection (Element 7)

H. Water Sampling and Monitoring (Element 8)



What has IRWA been doing to help us comply?

- Conducted a "pilot" using U.S. EPA software tools
- Conducted a "pilot" using proprietary software - SEMS
- Developed templates for RRA and ERP

Where do you go for help on the RRA and ERP?

- Go to IRWA website @:

https://www.ilrwa.org/ and follow links or

http://www.ilrwa.org/Downloads/VAERPhtml.html

Word and Excel versions.

- Pros and cons to both versions….
- Disclaimer – We did our best to make documents meet State and Federal Requirements. However, no legal review so….

Cyber-security

- Federal Push to Make Water Systems Institute Security because of ever increasing risk.
  - Probably didn't adequately address in ERP.
  - U.S. EPA trying to institute a requirement in Illinois EPA inspections
  - Push back from AWWA and NRWA
  - ULTIMATELY, WE WILL HAVE TO DO SOMETHING
    - It is a real problem

WHAT IS CYBERSECURITY

Cybersecurity is the practice of ensuring confidentiality, integrity, and availability of information by protecting your digital systems and networks from unauthorized access or usage.

- **Protection of Information Technology (IT) - the systems that collect, store, and process data (e.g. billing software)**
- **Protection of Operational Technology (OT) – the hardware or software that detects or cause a change, through direct monitoring of industrial equipment (e.g. SCADA)**

HOW ARE THE FEDS GOING TO GET THERE?

- **Ultimately Illinois EPA Inspectors will complete a checklist**
  - **Once the checklist is completed, a report will be generated that will be part of Attachment A**
    - **Once the report is generated water systems will be required to make corrective actions.**

(This approach has not been implemented; but, may be inevitable.)

Attachment "B" of Your Next IEPA Inspection

Cybersecurity continues to be an increasing threat to public water supplies. All water supplies should act to examine cyber security vulnerabilities and develop a cyber security risk management program. As part of this program, passwords should be routinely changed, software kept up to date, and regular screenings of security measures such as firewalls should be done. Guidance can be found at: https://www.epa.gov/waterresilience/cybersecurity-planning

In the event your system is hacked, immediately notify the United States Cybersecurity and Infrastructure Security Agency (CISA) at 888-282-0870, the Illinois Emergency Management Agency (IEMA) at 1-800-782-7860, and your local FBI Field Office https://www.fbi.gov/contact-us/field-offices Further information on reporting cyber-attacks can be found at: https://www.epa.gov/system/files/documents/2023-02/230202-CyberIncidentReportingProcess_21118.pdf

WHAT CAN WE DO PREPARE?

- **We have access to the checklist and can self-evaluate. (https://www.epa.gov/system/files/documents/2023-03/EPA%20Water%20Cybersecurity%20Assessment%20Tool%201.0_0.xlsx)**
  - **Begin now to work on resiliency and develop a plan to mitigate weaknesses identified in the self-assessment**
  - **Be prepared to show inspectors our self-assessment and mitigation plan (understand that making a copy for them is not a good idea because of FOIA)**
  - **Make Cybersecurity part of your EOP/ERP such that it will be continually evaluated**

WHAT CAN I DO WHEN I GET BACK FROM TRAINING?

- **Start biting this off in small portions. Start with the stuff that you can control.**
- **Focus on things in following areas:**
  - **Account Security**
  - **Device Security**
  - **Data Security**
  - **Vulnerability Management**
  - **Supply Chain**
  - **Response and Recovery**

ASK YOURSELF THE FOLLOWING?

Account Security

- **Do I use default passwords?**
  - **Don't continue using default passwords. If you can't change SCADA passwords, isolate the equipment and schedule to check logs for sign-ins.**
- **Do we require passwords to be changed and are they complex?**
  - **Enforce Password Length & Complexity- require all employees to create long and complex passwords that should at minimum be eight characters long and contain one uppercase letter, one lowercase letter, one number, one symbol.**
- **Do we require separate credentials for OT and IT?**
  - **Usernames and Passwords should be different for users who access both IT and OT networks.**

Device Security

- **Do I know what software and hardware I use on a regular basis?**
  - **An accurate inventory of IT and OT assets will help during the recovery phase of a cyber incident.**
  - **As part of your ERP/EOP indicate the amount of time needed to replace sensors and other equipment associated with SCADA.**
- **Can anyone load programs or devices onto the IT or OT system?**
  - **Unauthorized hardware should never be allowed to be connected to systems. This includes USB thumb drives, external hard drives, laptops, or cell phones.**
  - **Closely control administrative rights to control installation of software that could contain malware.**

Data Security

- **Do we have, collect and protect security logs?**
  - **Ensure logs are properly stored in a central system that can only be accessed by users who are both authorized and authenticated.**
- **Do we back up our critical information?**
  - **Critical IT and OT data should be backed up regularly and stored in a protected location off-site.**
- **Do we encrypt information stored?**
  - **Data encryption can help maintain the confidentiality of sensitive data and integrity of both IT and OT networks. Do not store any sensitive data in a plain text format and only allow access to sensitive data to authorized and authenticated use. Some programs (e.g., web browser) may do this without you even knowing.**

Vulnerability Management

- **Do we routinely update our programs and systems when upgrades are provided?**
  - **Identify and install updates/patches to reduce the likelihood of cybercriminals exploiting known vulnerabilities to breach a network.**
- **Do we limit internet access to OT/IT systems?**
  - **Ensure systems do not have unnecessary internet exposure and avoid connecting OT assets to the internet as much as possible.**

Supply Chain

- **When contracting IT or OT services or purchasing equipment/software do we consider security support or measures?**
  - **To protect your investment in IT and OT assets or services ensure that cybersecurity is an important evaluation criterion.**

Response/Recovery

- **What am I going to do if I have a security breach?**
  - **Create an Incident Response Plan that is part of your ERP/EOP. The plan should contain detailed procedures on how to respond to a cyber incident which can help minimize response and recovery times. If you have an incident update your plan after the incident.**
  - **To speed your recovery backup all systems that are necessary for operation on a schedule that will reduce the likelihood and duration of data loss and loss of operation. Store backups separately from source system and test regularly.**

Other Security Topics

- **Do I keep my OT separate from my IT?**
  - **If not, you need a barrier between the two systems, aka. a firewall. This firewall can help reduce the likelihood of the OT network being compromised if the IT network is compromised.**