Cybersecurity
& other threats

Patti Kay Wisniewski
Wisniewski.patti-kay@epa.gov
Water Works Operators Association of Pennsylvania
Boalsburg, PA
September 30, 2024

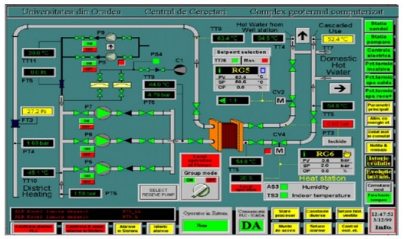


Figure 1 SCADA

Those who wish to do us harm

- National States for Geopolitical Reasons
- Hacktivists for Ideological Reasons
- Terrorist Groups for Ideological Violence
- Insider Threats due to Discontentment
- Cyber Criminals for Profits

OT and IT are concerns

Information Technology (IT)

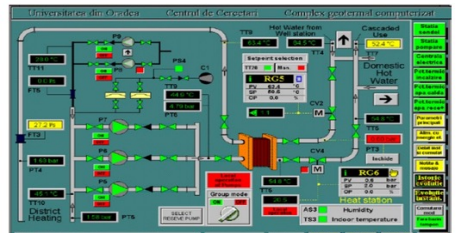
- use of hardware, software, services, and supporting infrastructure to manage and deliver information using voice, data, and video.

E.g. office computers, network switches, servers, firewalls

Operational Technology (OT)

- technology that uses a combination of software and hardware to monitor and control specific devices and processes in an industrial setting.

E.g. PLC, ICS, SCADA



Don't forget Physical Security

The threat is real, ever evolving

Water suppliers have been victims

NOT a once and done preparedness activity

Unknown Future of AI

Others are posing as EPA or CISA to mislead

Even the very basic actions are important

Proactive Steps for Protection

1. Reduce Exposure to the Public Facing Internet
2. Conduct Regular Cybersecurity Assessments
3. Change Default Passwords Immediately
4. Conduct an Inventory of OT/IT Assets
5. Develop/Exercise Incident Response/Recovery Plans
6. Backup OT/IT Systems
7. Reduce Exposure to Vulnerabilities
8. Conduct Cybersecurity Awareness Training

ALERT

Phone Scammers Impersonating CISA Employees

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

How to Protect Yourself

- Do not pay the caller!
- Take note of the phone number calling you.
- Hang up immediately.
- Validate the contact by calling CISA at (844) SAY-CISA (844-729-2472) or report it to law enforcement

Fraud Alert – EPA Office of Inspector General Issues Notice of Violation Phishing Scam

What To Do

EPA encourages recipients of any *suspicious* Notice of Violation letters to carefully examine the details, particularly the contact information, and to reach out directly to the EPA's enforcement office for verification.

NOTE: EPA fines are paid to the US Treasury

EPA RESILIENCE GRANTS

Safe Drinking Water Act Resilience Grants

The Safe Drinking Water Act Resilience Grants work to help public water systems increase their resilience to natural hazards and extreme weather events, and to reduce cybersecurity vulnerabilities. Projects that may receive funding include but are not limited to those that conserve water or enhance water use efficiency, improve drinking water infrastructure, design desalination facilities, or enhance water supply through watershed management and source water protection. Funds are available for public water systems through two separate grant programs.

Resilience Grants

Drinking Water System Infrastructure Resilience and Sustainability Program (SDWA 1459A(l)):

protecting drinking water sources from natural hazards, extreme weather events, and cybersecurity threats.

Midsize and Large Drinking Water System Infrastructure Resilience and Sustainability Program (SDWA 1459F):

Prepare for Cyber Incidents

- EPA Incident Action Checklist

https://www.epa.gov/waterresilience/cybersecurity-planning#IAC

- WaterISAC Resources
- Actions Recommended by CISA

TIP: Documentation!

1. Reduce Exposure to the Public Facing Internet
2. Conduct Regular Cybersecurity Assessments
3. Change Default Passwords Immediately
4. Conduct an Inventory of OT/IT Assets
5. Develop/Exercise Incident Response/Recovery Plans
6. Backup OT/IT Systems
7. Reduce Exposure to Vulnerabilities
8. Conduct Cybersecurity Awareness Training

FREE CYBER VULNERABILITY SCANNING FOR WATER UTILITIES

WATER SECTOR COORDINATING COUNCIL

Reach out:
vulnerability@cisa.dhs.gov

Plan for Response to Cyber Incidents

- Switch to manual operations, if feasible
- Test operations manually before you ever need to operate in this manner
- Prepare written procedures for manual operations and how to restore to full operations
- The quicker your system can identify and react to a threat, the less damage a cyberattack can cause

Report Cyber Incidents

State Police

CISA at 888-282-0870 or email at Report@cisa.gov

CISA provides technical assets and assistance to mitigate vulnerabilities, reduce the impact of the incident

PADEP Needs to know

EPA - work through me

Enforcement Alert: Drinking Water Systems to Address Cybersecurity Vulnerabilities

EPA Increases Enforcement Activities to Ensure Drinking Water Systems Address Cybersecurity Threats

Reminders--AWIA aka *SDWA Section 1433* Deadlines are approaching

CWS Size	R&R Assessment Certification	ERP Certification
≥ 100,000	March 31, 2025	September 30, 2025
50,000 - 99,999	December 31, 2025	June 30, 2026
3,301 - 49,999	June 30, 2026	December 31, 2026

https://www.epa.gov/waterresilience/awia-section-2013
www.epa.gov/waterresilience

What is required - Review of RRA

shall include:
1.the risk to the system from malevolent acts and natural hazards;
2.the 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;

TIP: Documentation!

What is required - Review of RRA

shall also include:
3. the monitoring practices of the system;
4. the financial infrastructure of the system;
5. the use, storage, or handling of various chemicals by the system; and
6. the operation and maintenance of the system

TIP: Documentation!

What is required - Review of ERP

The ERP shall include:
1.strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system;

2. 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;

TIP: Documentation!

What is required - Review of ERP

The ERP shall also include:
3. actions, procedures and equipment to significantly lessen the impact on public health and the safety and supply of drinking water, (alternative source water relocation of water intakes, construction of flood protection barriers); and

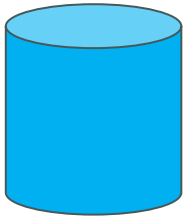
4. strategies that can be used to aid in the detection of malevolent acts or natural hazards that threaten the security or resilience of the system.

EPA interprets the population served to mean **all persons served** by the system directly or indirectly ….

community water systems should determine their population served based on the **number of people the system serves directly, PLUS** the **number of people served by any consecutive** water systems.

Population Served

Certifying your RRA and ERPs



- **Submit a certification** that the system has **reviewed** its assessment and, if applicable, **revised** such assessment

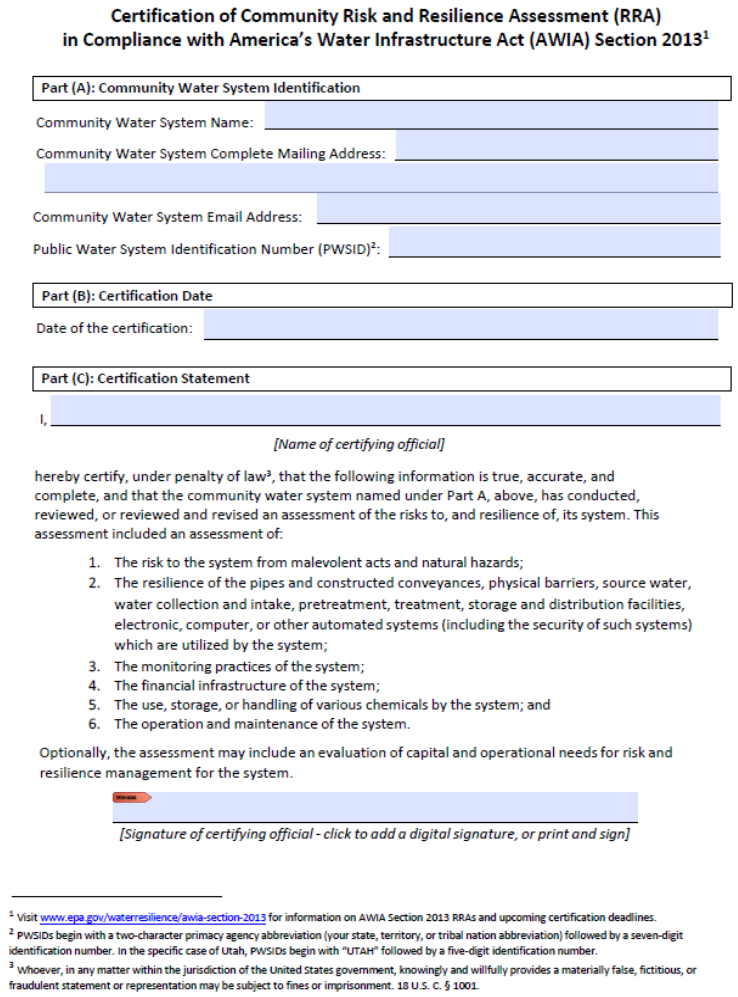
- **Submit a certification** that the system has **reviewed** its ERP and, if applicable, **revised** such plan

TIP: Documentation!

NEW

RRA & ERP Certification Forms

- ✓ Form Fillable
- ✓ Population Served
- ✓ PWSID# begin **PA**
- ✓ Reviewed *or* Reviewed/Revised



Certification of Community Risk and Resilience Assessment (RRA) in Compliance with America's Water Infrastructure Act (AWIA) Section 2013[1]

Part (A): Community Water System Identification

Community Water System Name:

Community Water System Complete Mailing Address:

Community Water System Email Address:

Public Water System Identification Number (PWSID)[2]:

Part (B): Certification Date

Date of the certification:

Part (C): Certification Statement

I,

[Name of certifying official]

hereby certify, under penalty of law[3], that the following information is true, accurate, and complete, and that the community water system named under Part A, above, has conducted, reviewed, or reviewed and revised an assessment of the risks to, and resilience of, its system. This assessment included an assessment of:

1. The risk to the system from malevolent acts and natural hazards;
2. The 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;
3. The monitoring practices of the system;
4. The financial infrastructure of the system;
5. The use, storage, or handling of various chemicals by the system; and
6. The operation and maintenance of the system.

Optionally, the assessment may include an evaluation of capital and operational needs for risk and resilience management for the system.

[Signature of certifying official - click to add a digital signature, or print and sign]

[1] Visit www.epa.gov/waterresilience/awia-section-2013 for information on AWIA Section 2013 RRAs and upcoming certification deadlines.

[2] PWSIDs begin with a two-character primacy agency abbreviation (your state, territory, or tribal nation abbreviation) followed by a seven-digit identification number. In the specific case of Utah, PWSIDs begin with "UTAH" followed by a five-digit identification number.

[3] Whoever, in any matter within the jurisdiction of the United States government, knowingly and willfully provides a materially false, fictitious, or fraudulent statement or representation may be subject to fines or imprisonment. 18 U.S. C. § 1001.

EPA Resources for Cybersecurity Enhancements!

Don't get distracted when other things are happening

Obtain a *FREE* assessment from EPA and receive a cyber action plan; learn best practices

https://www.epa.gov/waterresilience/epa-cybersecurity-water-sector

Free Onsite Cybersecurity Assessment and Technical Assistance

Cybersecurity is a broad term that refers to the security of computer network infrastructure and data. A cyber attack is an attempt to undermine or compromise the function of a computer network or system, or an attempt to track the online movements of individuals without their permission.

What is the onsite assessment and technical assistance?

With the U.S. Environmental Protection Agency, Horsley Witten Group (HWG) is offering free, confidential, onsite cybersecurity assessments and technical assistance to interested water and wastewater utilities. The assessment consists of a questionnaire completed on-site with HWG staff, and the technical assistance consists of developing a cyber action plan based on the results of your utility's assessment focused on best practices to prepare for, respond to, and recover from a cyber incident. Adoption of these practices can reduce the likelihood that a cyber attack will be successful and allow the utility to recover from any cyber attacks faster and at a lower cost.

What are the expected outcomes?

All individual utility information gathered during the assessment will be protected and remain confidential. Trends in the anonymized, aggregated data will be shared with other utilities and agencies so that lessons learned from the assessments may benefit all.

Participating utilities can expect to receive a straightforward overview of their vulnerabilities and suggested best practices to reduce risks to their business enterprise, SCADA, and communications systems. Additionally, the utility will develop their cyber action plan with HWG and work to implement any recommended best practices.

What does the utility need to prepare before the onsite assessment and technical assistance?

The assessment will require input from management, IT, operations/control staff and engineers as appropriate. The utility will also need to compile and provide any existing system documentation/diagrams, policies, and procedures.

Is there any follow-up?

Yes, HWG will contact the utility on two separate occasions after the development of the cyber action plan to gauge progress and see if additional assistance is required.

To register your utility, please visit:
https://horsleywitten.com/cybersecurityutilities

For more information, contact:
Gemma Kite at **508-833-6600**

Horsley Witten Group
Sustainable Environmental Solutions
horsleywitten.com

EPA

Be Aware of other Threats

- Damage to electric grid impacting water and interdependencies
- Mis-information (incorrect)
- Dis-information (intentional to mislead, China during US disasters to further disrupt, fear)
- Insider Threats / anything connected to your network
- Wildfires / climate change impacts
- CrowdStrike
- Physical Tampering

Questions?

Patti Kay Wisniewski
Wisniewski.patti-kay@epa.gov
215.514.7893

Get on my email group to always hear the latest from EPA