

Threats to Critical Infrastructure

Joint Conference of SE District - PA AWWA
and the Eastern Section WWOAP

Patti Kay Wisniewski

Wisniewski.patti-kay@epa.gov

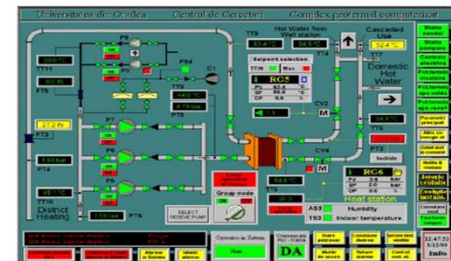


Figure 1 SCADA



KATRINA

CAT 3
125 MAX WINDS
DIAMETER: 400 MILES
WIND FIELD: 230 MILES



HELENE

CAT 4
140 MAX WINDS
DIAMETER: 822 MILES
WIND FIELD: 370 MILES



KATRINA

CAT 3
125 MAX WINDS
DIAMETER: 400 MILES
WIND FIELD: 230 MILES



HELENE

CAT 4
140 MAX WINDS
DIAMETER: 822 MILES
WIND FIELD: 370 MILES



Katrina 2025

Deaths = 1,392

Damages \$125 Billion

Helene 2024

Deaths = > 220

Damages = > \$30 Billion

WHITE HOUSE ANNOUNCES CYBERSECURITY AWARENESS MONTH



President Biden declared **October 2024** to be Cybersecurity Awareness Month.

The White House and the Biden Administration hope to encourage agencies and states to take action to protect people, businesses, and infrastructure from the increasing cyber threats.



Those who wish to do us harm



National States for Geopolitical Reasons

Hacktivism 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.

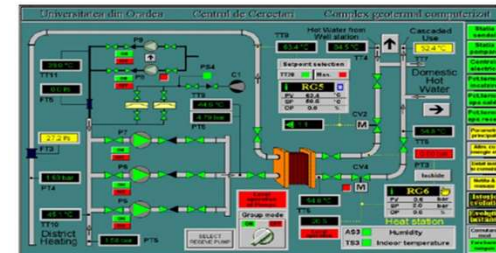
E.g. office computers, network switches, servers, firewalls

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

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**



America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

[Topics](#) ▾ [Spotlight](#) [Resources & Tools](#) ▾ [News & Events](#) ▾ [Careers](#) ▾ [About](#) ▾

[Home](#) / [News & Events](#) / [Cybersecurity Advisories](#) / [Alert](#)

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.



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(I)):



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

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

Prepare for Cyber Incidents

- EPA Incident Action Checklist

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

- WaterISAC Resources
- Actions Recommended by CISA

TIP: Documentation!





Top Cyber Actions for Securing Water Systems

TLP:CLEAR

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.

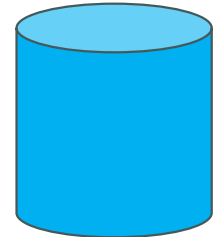
EPA interprets the population served to mean **all persons served** by the system directly or indirectly

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!





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 2013¹**

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 law³, 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 primary 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/water-resilience/epa-cybersecurity-water-sector>



Free Onsite Cybersecurity Assessment and Technical Assistance

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 Tools and Resources

<https://www.epa.gov/water-resilience/epa-cybersecurity-water-sector>



Water Security is National Security



FACT SHEET

EPA's Cybersecurity Resources for Drinking Water and Wastewater Systems

Improving cybersecurity across the water sector remains one of EPA's highest priorities. EPA continues to underscore that adopting cybersecurity best practices at drinking water and wastewater utilities is essential to protect communities from the increasing number and severity of cyber-threats facing our nation's water systems. The Agency will continue to explore opportunities to lower cybersecurity risk for public water systems.

EPA will continue to support states, technical assistance providers, drinking water and wastewater systems by providing ongoing technical assistance in the form of cybersecurity assessments, subject-matter expert consultations, training, and funding.

Cybersecurity Assessments

EPA conducts cybersecurity assessments for utilities through the [Cybersecurity Evaluation Program](#) where utilities work with a cybersecurity professional virtually to complete an assessment using the WCAT, described below. Following the assessment, utilities will receive their comprehensive Assessment Report and Risk Mitigation Plan Template so they can begin addressing their cybersecurity gaps and track their progress as they make improvements to their cybersecurity program.

EPA's [Water Cybersecurity Assessment Tool \(WCAT\)](#) helps water systems self-assess their cybersecurity practices. State Primacy Agencies and Technical Assistance Providers can also use this tool when conducting a cybersecurity assessment at water systems. The tool utilizes [EPA's Cybersecurity Checklist](#), which contains the basic cybersecurity controls needed to build a strong cybersecurity program.

Cybersecurity Technical Assistance

EPA offers direct technical assistance through the [Cybersecurity Technical Assistance Program for the Water Sector](#). Primacy agencies, technical assistance providers, and utilities can submit cybersecurity questions and receive one-on-one remote assistance (phone or email) from a cybersecurity subject-matter expert. EPA strives to respond to each request for technical assistance within two business days. Using EPA's [Cybersecurity Checklist Fact Sheets](#), for each of the 33 questions on the WCAT, utilities can learn additional details on each cybersecurity control including why it's important, recommendations, implementation tips (corrective actions), and additional resources utilities can access to assist in implementing each control.

Cybersecurity Training

EPA offers cybersecurity training and tabletop exercises free to the water sector. For example, [EPA's Cybersecurity 101 Webinar](#) introduces the basic principles of cybersecurity to Water Sector members. EPA has also conducted trainings on how to use the WCAT to conduct cybersecurity assessments at water and wastewater utilities for technical assistance providers and water systems. EPA also hosts webinars covering cybersecurity concepts and highlighting EPA's cybersecurity assessment resources for water systems supporting Defense drinking water and wastewater facilities.

Working in coordination with states, State-Level Rural Water Sections and Water/Wastewater Agency Response Networks (WARNs), EPA hosts tabletop exercises featuring scenarios that allow staff to assess their cyber response practices, identify ways to improve their cybersecurity posture, and engage with cybersecurity subject-matter experts.

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

