



CYBERSECURITY AND INCIDENT RESPONSE PLANNING

Office of Drinking Water



Our Office's work supports the vision and mission of the Department of Health.

OFFICE OF DRINKING WATER

Vision

The Office of Drinking Water supports our communities to address competing water challenges, such as climate change, water resources, aging infrastructure, and economic development. We ensure and promote the value of safe and reliable drinking water to all people of Washington, now and for generations to come.

Mission

The Office of Drinking Water works with others to protect the people of Washington by ensuring safe and reliable drinking water.

WASHINGTON STATE DEPARTMENT OF HEALTH

VISION • MISSION • VALUES

VISION

Equity and optimal health for all

MISSION

The Department of Health works with others to protect and improve the health of all people in Washington State.

VALUES

Our values describe who we are and who we need to become.

Human-centered — We see others as people who matter like we do and take into account their needs, challenges, contributions and objectives.

Equity — We are committed to fairness and justice to ensure access to services, programs, opportunities, and information for all.

Partnership and Collaboration — We seek partnership and collaboration to maximize our collective impact. We cannot achieve our vision alone.

Seven Generations — Inspired by Native American cultures, we seek wisdom from those who came before us to ensure our current work protects those who will come after us.

Excellence — We strive to demonstrate best practices, high performance, and compelling value in our work every day.





MISSION

We work with others to protect the health of the people of Washington by ensuring safe and reliable drinking water.

VISION

The people of Washington understand the value of safe and reliable drinking water to healthy communities and a vibrant economy. As a result, our public water systems have the technical, managerial, and financial capacity they need to provide it, now and for generations to come.

VALUES

Collaboration
Respect
Accountability

Learning
Compassion
Diversity

Commitment
Innovation
Empowerment

ROLES

- ◆ Respond to public health emergencies related to drinking water
- ◆ Set clear expectations for Washington's public water systems and hold them accountable for protecting public health
- ◆ Provide funding and technical assistance to support safe and reliable drinking water
- ◆ Educate and inform our partners and the people of Washington about drinking water issues



Presenter



Kim Moore

Manager

Engineering & Technical Services Section

Kimberly.Moore@doh.wa.gov

[Drinking Water Systems](#) | [Washington State Department of Health](#)



@WADeptHealth

DOH Strategic Plan



What We Do

Ensure public safety
Create the healthiest next generation
Promote healthy living and healthy aging



How We Do Our Work

Serve our customers and continue to improve
Be efficient, innovative and transparent
Develop and support our workforce



Guiding Principles

Evidence-based public health practice
Partnership
Transparency
Health equity
Seven generations



Vision

People in Washington enjoy longer and healthier lives because they live in healthy families and communities.



Strategy

Through collaborations and partnerships, we will leverage the knowledge, relationships and resources necessary to influence the conditions that promote good health and safety for everyone.



Mission

The Department of Health works with others to protect and improve the health of all people in Washington.

Agenda

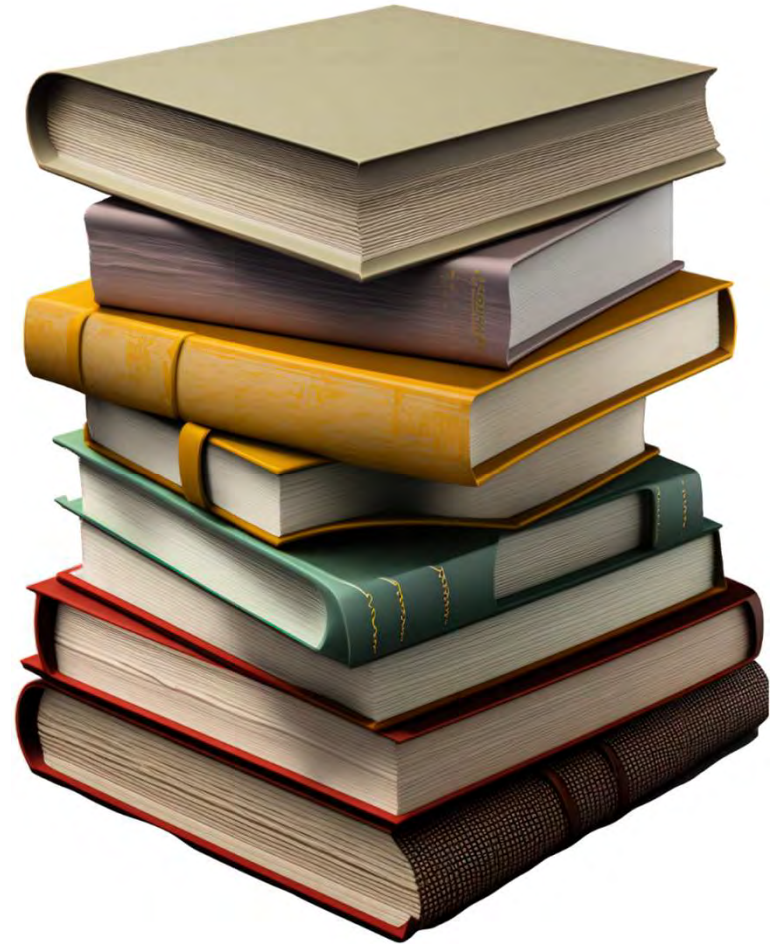
- Overview of Current Cybersecurity Planning Requirements
- Overview of Future Cybersecurity Planning Requirements
- Overview of Cybersecurity in the Water Sector
 - Importance of Cybersecurity
 - Incident Response Plans
 - Resources for Funding

Background

- Critical infrastructure is becoming increasingly the target of cyber attack campaigns from advanced persistent threats (APTs). These are often nation-state sponsored organizations.
- Drinking water infrastructure is particularly vulnerable as they often have minimal cybersecurity measures in place compared to other critical infrastructure sectors.
- National Security Council (NSC) sent a letter to all Governors on March 28, 2024, requesting they submit a plan to routinely and methodically address cybersecurity vulnerabilities by June 28, 2024.

Current Cybersecurity Planning Requirements

America's Water Infrastructure
Act (AWIA)



AWIA Overview

- Water and Wastewater Systems are designated as critical infrastructure, as defined by law ([Homeland Security Act of 2002](#)).
- Water and Wastewater Systems staffers are first responders ([6 U.S.C.101\(6\)](#), [HSPD-8](#), [DHS CERRA Guidance](#), and [APWA](#)).
- Tampering with a Water System is a Federal Offense ([Safe Drinking Water Act](#)).
 - Penalties up to 20 years in prison and \$1,000,000 fine.
 - Attempting to tamper with a water system carries penalties of up to 10 years in prison and \$100,000 fine.

Introduction to AWIA

- America's Water Infrastructure Act ([AWIA](#)) was passed by Congress and signed into law by the president on October 23, 2018.
- Community Water Systems serving more than 3,300 persons are required to do the following:
 - Conduct Risk and Resilience Assessment (RRA)
 - Prepare or Revise Emergency Response Plan (ERP)
 - Submit Certification Letter to EPA for each
 - Review and update both items every 5 years
 - Record maintenance

Required Assessments Under AWIA

- Malevolent Acts
- Natural Hazards
- All critical Components of the System
- Monitoring Practices of the System
- Financial Infrastructure
- Use, storage, or handling of various chemicals
- Operation and maintenance of the system
- Capital and Operational needs for risk and resilience management

Emergency Response Plans (ERPs)

AWIA Requirements for Elements of ERPs:

- Strategies to improve resilience, including physical and cyber security.
- Plans, procedures and equipment to be utilized in all hazards response.
- Actions, procedures, equipment to lessen impact on public health.
- Strategies for detection of emergencies.

AWIA Compliance Deadlines

Deadlines for Certification of Completion to EPA:

Population Served	Previous RRA Deadline	Next 5-Year Submission Cycle RRA Deadline
≥100,000	March 31, 2020	March 31, 2025
50,000-99,999	December 31, 2020	December 31, 2025
3,301-49,999	June 30, 2021	June 30, 2026



Population Served	Previous ERP Deadline*	Next 5-Year Submission Cycle ERP Deadline*
≥100,000	September 30, 2020	September 30, 2025
50,000-99,999	June 30, 2021	June 30, 2026
3,301-49,999	December 31, 2021	December 31, 2026

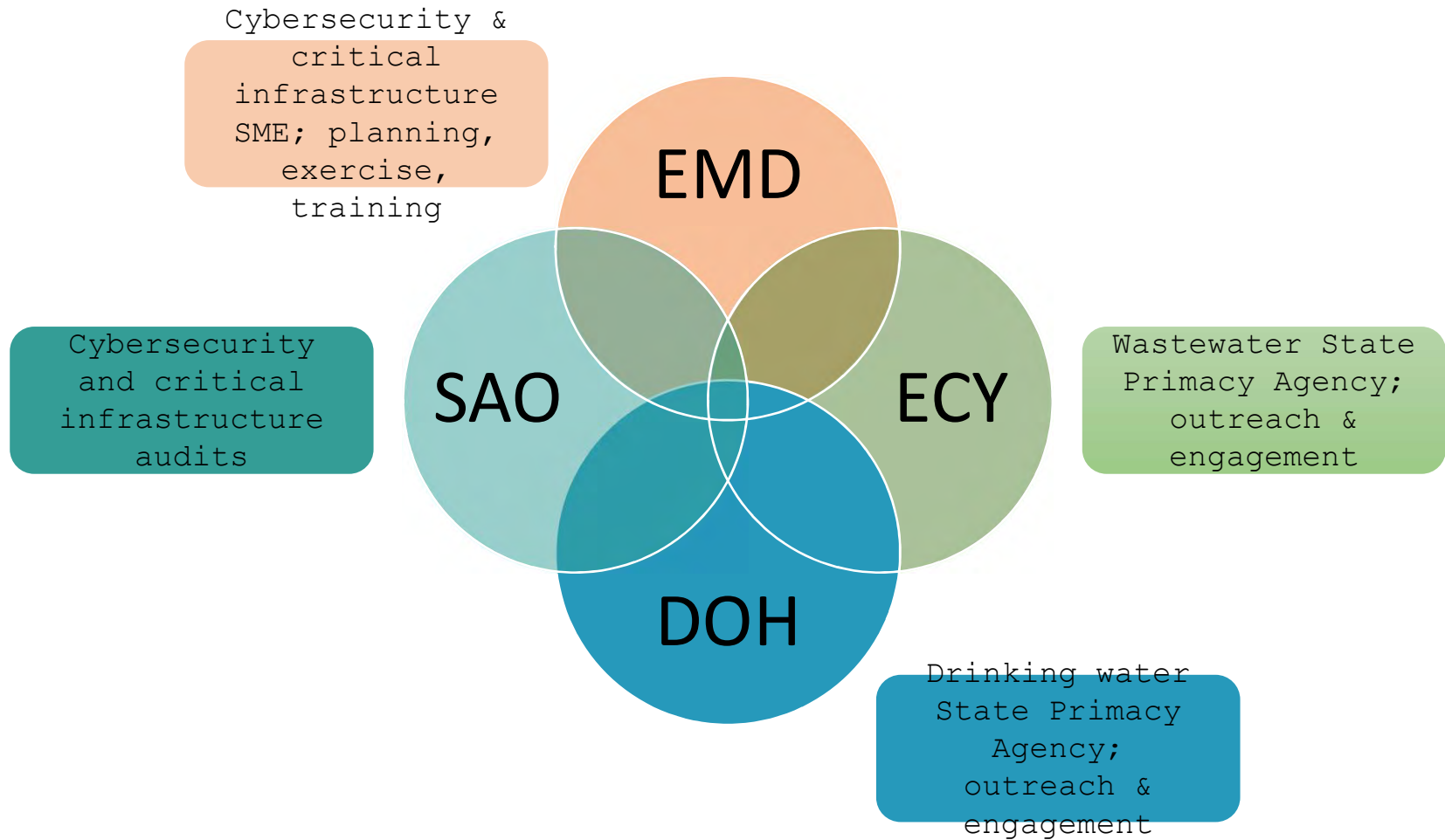
[Enforcement Alert: Drinking Water Systems to Address Cybersecurity Vulnerabilities | US EPA](#)

Future Cybersecurity Planning Requirements

State Cybersecurity Action Plan
for the Water Sector



Collaborative Approach



Scope



Drinking water
systems:

Community
Drinking Water
Systems that meet
the EPA
definition for
medium, large,
and very large
systems

Wastewater
Treatment
Plants:

Facilities
that meet EPA
definition for
major (>1MGD)

**Total systems
/ facilities
in scope**

Cybersecurity Action Plan

Strongly Encouraged Activities of Water Utilities Serving Populations Greater Than 3,300 Persons:

- Cybersecurity Vulnerability Assessments
- Mitigation measures to address critical vulnerabilities
- Cybersecurity Incident Response Plans
- Water utilities to routinely update Vulnerability Assessments and Incident Response Plans

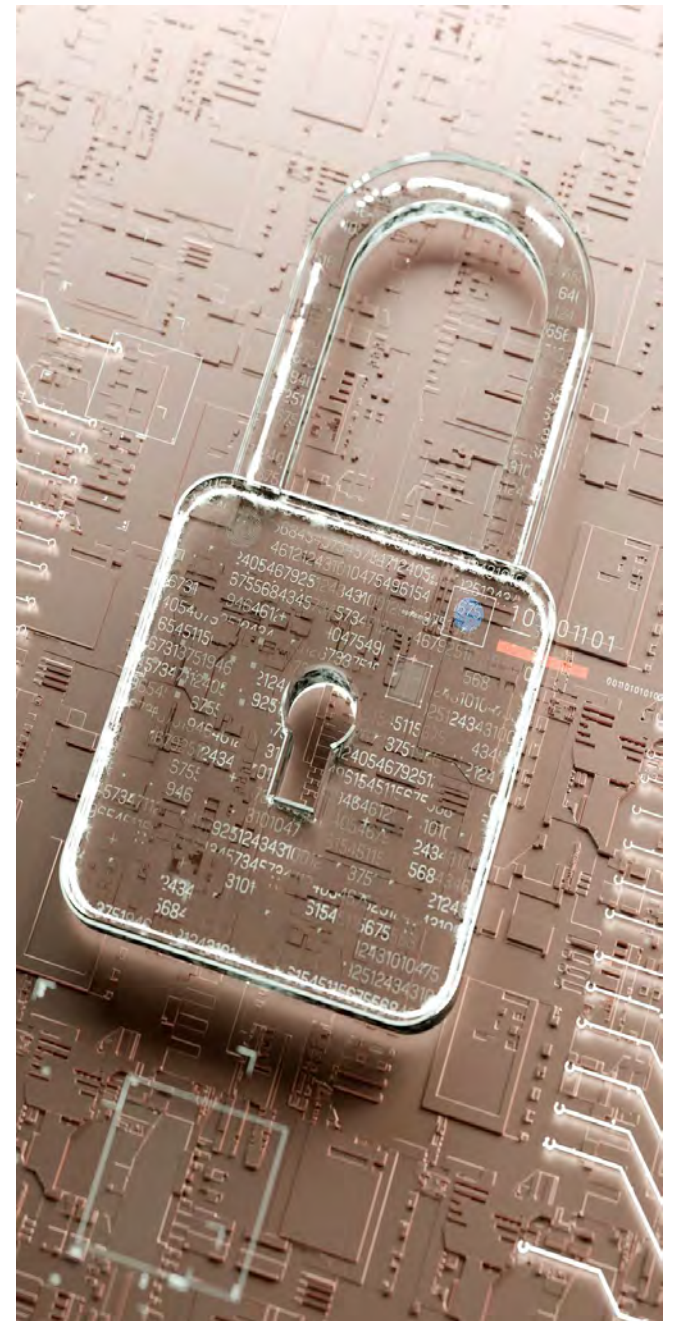
Cybersecurity Action Plan (Continued)

Implementation Strategies

- Outreach and engagement
- Raise awareness of State Auditor's Office (SAO) and Cybersecurity and Infrastructure Security Agency (CISA) audit opportunities
- Raise awareness of CISA, Environmental Protection Agency (EPA), and American Water Works Association (AWWA) free self assessment tools
- Provide resources for technical assistance
- Provide information regarding state and federal funding opportunities

Cybersecurity Overview

- Importance of Cybersecurity
- Cybersecurity Response Planning
- Cybersecurity Training
- Cybersecurity Funding Opportunities



Importance of Cybersecurity

- Cyber attacks could negatively impact public health
- Cyber attacks could cause service disruptions
- Cyber attacks could cause disclosure of employee or customer personally identifiable information (PII)
- America's Water Infrastructure Act (AWIA) compliance
- Cyber attacks could cause loss of public confidence and trust



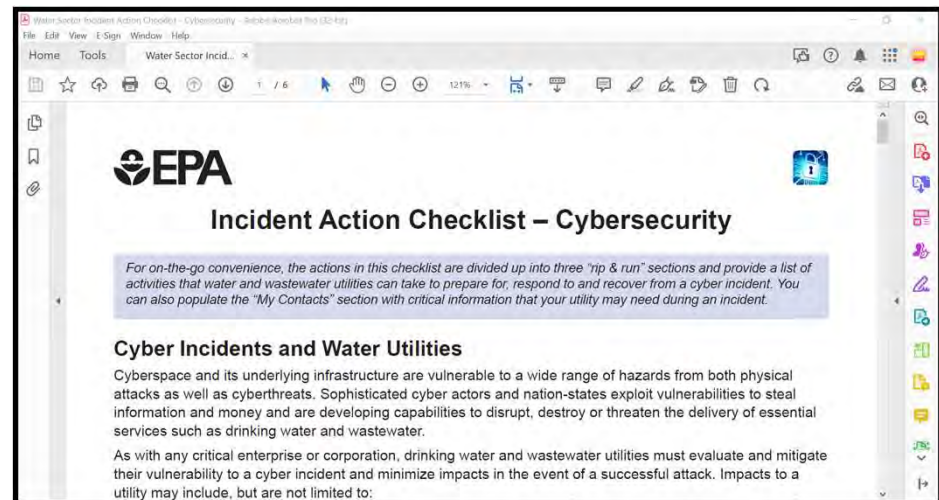
Common Cybersecurity Threats to Water Systems

- Phishing
- Outdated operating systems and software
- Control system devices with vulnerable firmware versions
- Cyber Intrusions
 - Insider threat
 - Ransomware attacks



EPA Cybersecurity Incident Action Checklist

- EPA Cybersecurity Incident Action Checklist is a great tool that can help your utility prepare for, respond to, and recover from cybersecurity incidents.
- [Water Sector Incident Action Checklist - Cybersecurity \(epa.gov\) - https://www.epa.gov/sites/default/files/2017-11/documents/171013-incidentactionchecklist-cybersecurity_form_508c.pdf](https://www.epa.gov/sites/default/files/2017-11/documents/171013-incidentactionchecklist-cybersecurity_form_508c.pdf)



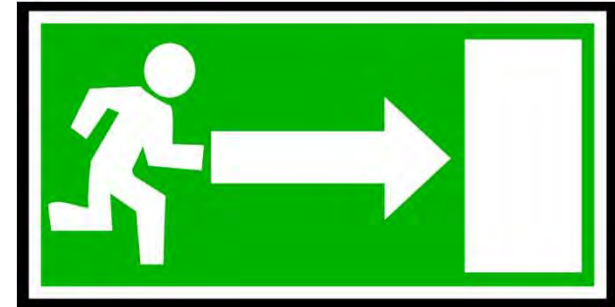
Incident Response Plan Key Elements

1. Basic system information.
2. Chain of Command—lines of authority (name, title, responsibilities, and contact numbers).
3. List of cyber events that qualify as emergencies.
4. Emergency notification list—other government agencies, priority customers, media, repair entities, neighboring water systems, etc.
5. Contact information for vendor who installed IT systems.
6. Contact information for vendor who installed and configured OT systems to include after hours contact information.
7. Designated spokesperson(s) (primary and alternate).







Incident Response Plan Key Elements *(Continued)*

8. Response actions for specific events:

- Power outage.
- Treatment equipment failure.
- Pump failure.
- Microbial contamination.
- Chemical contamination.
- Water service outages.
- Ransomware attack.
- Inability to contact customers.
- Inability to conduct business office functions such as billing or ordering of supplies.
- Unwanted disclosure of employee and/or customer PII.
- Provisions for Manual Operations



Incident Response Plan Key Elements *(Continued)*

- 9. Alternative water sources.
- 10. Alternate method to purchase supplies and services.
- 11. Sampling plan.  
- 12. Communication plan.  
- 13. Steps to return to normal operations.  
- 14. Plan approval—information regarding when and whom approved the emergency response plan.

Opportunities for Collaboration

- Assessment of Hazards in a Jurisdiction.
- Notification requirements of water systems and jurisdiction.
- Discussions to achieve understanding of interdependencies between water sector and other essential services.
- Discussions surrounding prioritization for restoration of water services.
- Discussion of water sector's resource needs to get back on-line.



Cybersecurity Response



- When to report a Cybersecurity Incident
- What information to Report
- Entities Cybersecurity Incidents should be Reported To

When to Report Cybersecurity Incidents

- Utilities are strongly encouraged to report all cybersecurity incidents as soon as they are discovered when there is any of the following:
 - Loss of data, system availability, or control of systems
 - Impact to victims
 - Detection of unauthorized access to critical information technology systems
 - Detection of malicious software presence in critical information technology systems
 - Affected critical infrastructure or core government functions
 - Impact to national security, economic security, or public health and safety

What Information to Report Regarding a Cybersecurity Incident

- Cybersecurity incidents can and should be reported even when full information is not known. Helpful information includes:
 - Name of water system and point(s) of contact
 - Who experienced the incident
 - What type of incident occurred
 - Specific details of impact of incident
 - How and when the incident was detected
 - What response actions have already been taken
 - Help needed (if known)
 - Whom else has already been notified

Entities a Cybersecurity Incident Should Be Reported To

- Washington State Department of Health – Office of Drinking Water
 - [ODW Headquarters](#) 360-236-3100
 - [Eastern Regional Office](#) 509-329-2100
 - [Northwest Regional Office](#) 253-395-6750
 - [Southwest Regional Office](#) 360-236-3030
 - After Hours Emergency Line for Water Utility Staff Only: 1-877-481-4901
- Washington State Department of Ecology – Wastewater Treatment Works
 - Andy O'Neill at (509) 710-3676 or aone461@ecy.wa.gov
- Washington State Patrol



Entities a Cybersecurity Incident Should Be Reported To (Continued)

- CISA – For Asset Response. CISA can provide technical assets and assistance to mitigate vulnerabilities and reduce the impact of the incident. Incident Reporting System at www.us-cert.cisa.gov/forms/report. CISA can be contacted by phone at 888-282-0870 and by email at Central@cisa.gov.
- EPA: Centralized Response. EPA's Water Infrastructure and Cyber Resilience Division (WICRD) will act as a federal single point of contact and coordinate the response. EPA WICRD can be reached at WICRD-outreach@epa.gov.



Cybersecurity Training Opportunities

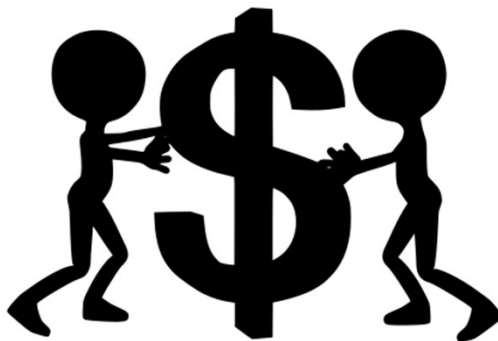
- EPA Cybersecurity 101 Webinar: [Cybersecurity 101 Webinar Slides \(pdf\)](#)
- CISA: [FedVTE](#): Free virtual training to gain a better understanding of cybersecurity.
- CISA: [Incident Response Training](#)
- CISA: [Industrial Control System Cybersecurity Training](#): Free training that provides information on cybersecurity for industrial control systems.
- Idaho National Laboratory: [Cyber-Informed Engineering](#)

Knowledge
is
power!



Cybersecurity Funding Opportunities

- Drinking Water State Revolving Fund
- Clean Water State Revolving Fund
- CISA State and Local Cybersecurity Grant Program



Drinking Water State Revolving Fund

- Drinking Water State Revolving Fund:
 - Provides assistance with All-Hazard Risk and Resilience Assessment, Equipment, and Infrastructure, including cybersecurity.
 - More information is available on the website: [Drinking Water State Revolving Fund \(DWSRF\) | Washington State Department of Health](#).
 - Point of contact: Washington State Department of Health: Applications and general questions—DWSRF@DOH.WA.GOV.



Clean Water State Revolving Fund

- Clean Water State Revolving Fund
 - Provides financial assistance to public, private, or nonprofit entities regarding measures to increase the security of publicly owned treatment works, including cybersecurity.
 - Point of Contact: Washington State Department of Ecology, Andy O'Neill at (509) 710-3676 or aone461@ecy.wa.gov. Or [Water quality grants and loans - Washington State Department of Ecology](#)



CISA State and Local Cybersecurity Grant Program

- CISA State and Local Cybersecurity Grant Program:
 - Grant program for states, cities, counties and towns from state administrative agency. Sub-award applications for cities, counties and towns must be submitted to the respective state agency.
 - For more information: [State and Local Cybersecurity Grant Program | CISA](#)
 - Point of Contact: FEMA has assigned state-specific Preparedness Officers for the SLCGP. Centralized Scheduling and Information Desk at (800) 368-6498 or email at askcsid@fema.dhs.gov.

Other Funding Opportunities

- Funding Programs for Drinking Water and Wastewater Critical Infrastructure Projects – Updated March 3, 2024

[Summary of Government Grant and Loan Programs for Water and Wastewater Projects](#)

Department of Health



Disease Control & Health Statistics

Initiatives

Measles Control
EndAIDS
Vital Statistics
(E. coli, mumps, etc.)



Environmental Public Health

Initiatives

Puget Sound Cleanup
PFAS
Pesticide Exposures



Prevention and Community Health

Initiatives

Tobacco 21
Immunization Rates
Family Planning (Title X)
Marijuana Prevention



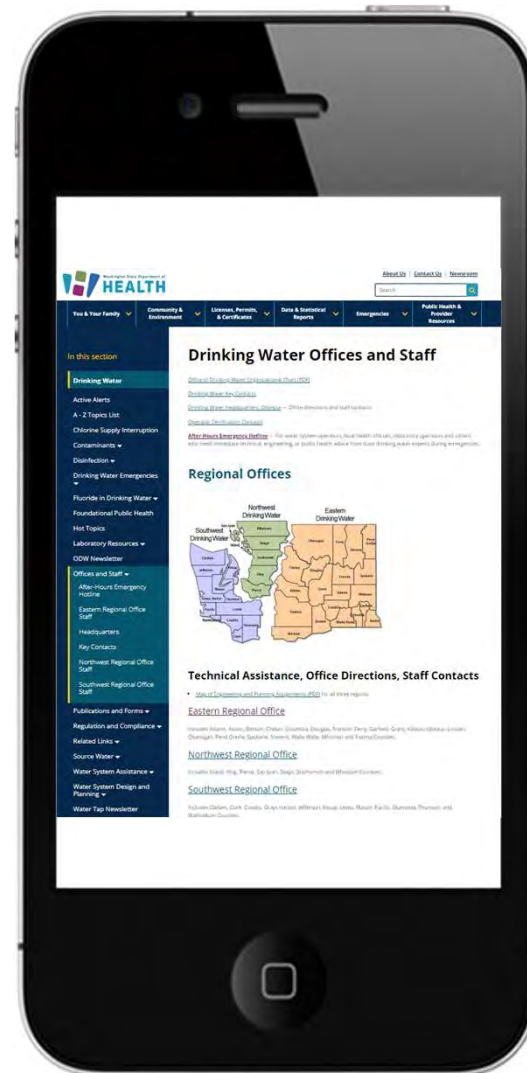
Health Systems Quality Assurance

Initiatives

Opioids
Behavioral Health Integration
Certificate of Need
Health Professions

Washington State Department of Health Office of Drinking Water

<https://doh.wa.gov/community-and-environment/drinking-water>



Questions?

Points of Contact



Kim Moore

Manager

Engineering & Technical Services Section

Kimberly.Moore@doh.wa.gov

<https://doh.wa.gov/community-and-environment/drinking-water>



@WADeptHealth



To request this document in another format, call 1-800-525-0127. Deaf or hard of hearing customers, please call 711 (Washington Relay) or email civil.rights@doh.wa.gov.

Resources



Cybersecurity Planning

- EPA: Cybersecurity Incident Action Checklist
https://www.epa.gov/sites/default/files/2017-11/documents/171013-incidentactionchecklist-cybersecurity_form_508c.pdf
- Other U.S. Government and Partner Cybersecurity Resources
 - [CISA Services Catalog](#) offers significant resources, guidance, and tools to assist critical infrastructure facilities, including water and wastewater systems, with cybersecurity.
 - [Industrial Control Systems Cybersecurity Initiative \(pdf\)](#) (178.16 KB): Considerations for ICS/OT Monitoring Technologies with an Emphasis on Detection and Information Sharing.

Cybersecurity Planning (Continued)

- Other U.S. Government and Partner Cybersecurity Resources (Continued)
 - [Presidential Policy Directive 41](#): Information on roles that government agencies will perform in the event of a cybersecurity incident.
 - [United States Department of Agriculture \(USDA\) Rural Development Circuit Rider Program](#)
 - [Water Information Sharing and Analysis Center \(WaterISAC\)](#)
 - [Multi-State ISAC](#)

Resources for Conducting Cybersecurity Risk Self Assessments

- Environmental Protection Agency (EPA): Water Cybersecurity Assessment Tool and Risk Mitigation Template
<https://www.epa.gov/system/files/documents/2023-03/EPA%20Water%20Cybersecurity%20Assessment%20Tool%201.0.0.xlsx>
- EPA: Guidance on Evaluating Cybersecurity During Public Water System Sanitary Surveys
https://www.epa.gov/system/files/documents/2023-03/230228_Cyber%20SS%20Guidance_508c.pdf
- Cybersecurity and Infrastructure Security Agency (CISA): Cyber Resilience Review
<https://www.cisa.gov/resources-tools/services/cyber-resilience-review-crr>

Resources for Conducting Cybersecurity Risk Assessments

Self Assessments (Continued)

- CISA: Cross-Sector Cybersecurity Performance Goals
https://www.cisa.gov/sites/default/files/2023-01/cisa_cpg_checklist_12052022.pdf
- CISA: Cybersecurity Evaluation Tool
<https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr>
- National Institute for Science and Technology (NIST): AXIO Cybersecurity Program Assessment Tool
<https://learn.axio.com/free-tool>

Resources for Conducting Cybersecurity Risk Assessments

Self Assessments (Continued)

- Multi-State Information Sharing and Analysis Center (MS-ISAC): Risk Assessment Method

<https://learn.cisecurity.org/cis-ram>



- MS-ISAC: Critical Security Controls

https://learn.cisecurity.org/cis-controls-download?_gl=1*72cofo*_ga*MTI3NTAyNzA3My4xNjgzOTExMzQx*_ga_N70Z2MKMD7*MTY4NDc3OTQwMC4zLjEuMTY4NDc3OTQwMS41OS4wLjA

Resources for Conducting Cybersecurity Risk Third Party Assessments

- EPA: Water Sector Cyber Security Evaluation Program
<https://www.epa.gov/waterriskassessment/forms/epas-water-sector-cybersecurity-evaluation-program>
- CISA: CISA Cybersecurity Advisor
<https://www.cisa.gov/about/regions>



Resources for Technical Assistance

EPA: Cybersecurity Technical Assistance Program for the Water Sector

<https://www.epa.gov/waterresilience/forms/cybersecurity-technical-assistance-program-water-sector>

EPA: Water Sector Cybersecurity Evaluation Program

<https://www.epa.gov/waterresilience/forms/epas-water-sector-cybersecurity-evaluation-program>

CISA Region X

<https://www.cisa.gov/water>

USDA Rural Development Circuit Rider Program

<https://www.rd.usda.gov/programs-services/water-environmental-programs/circuit-rider-program-technical-assistance-rural-water-systems>
