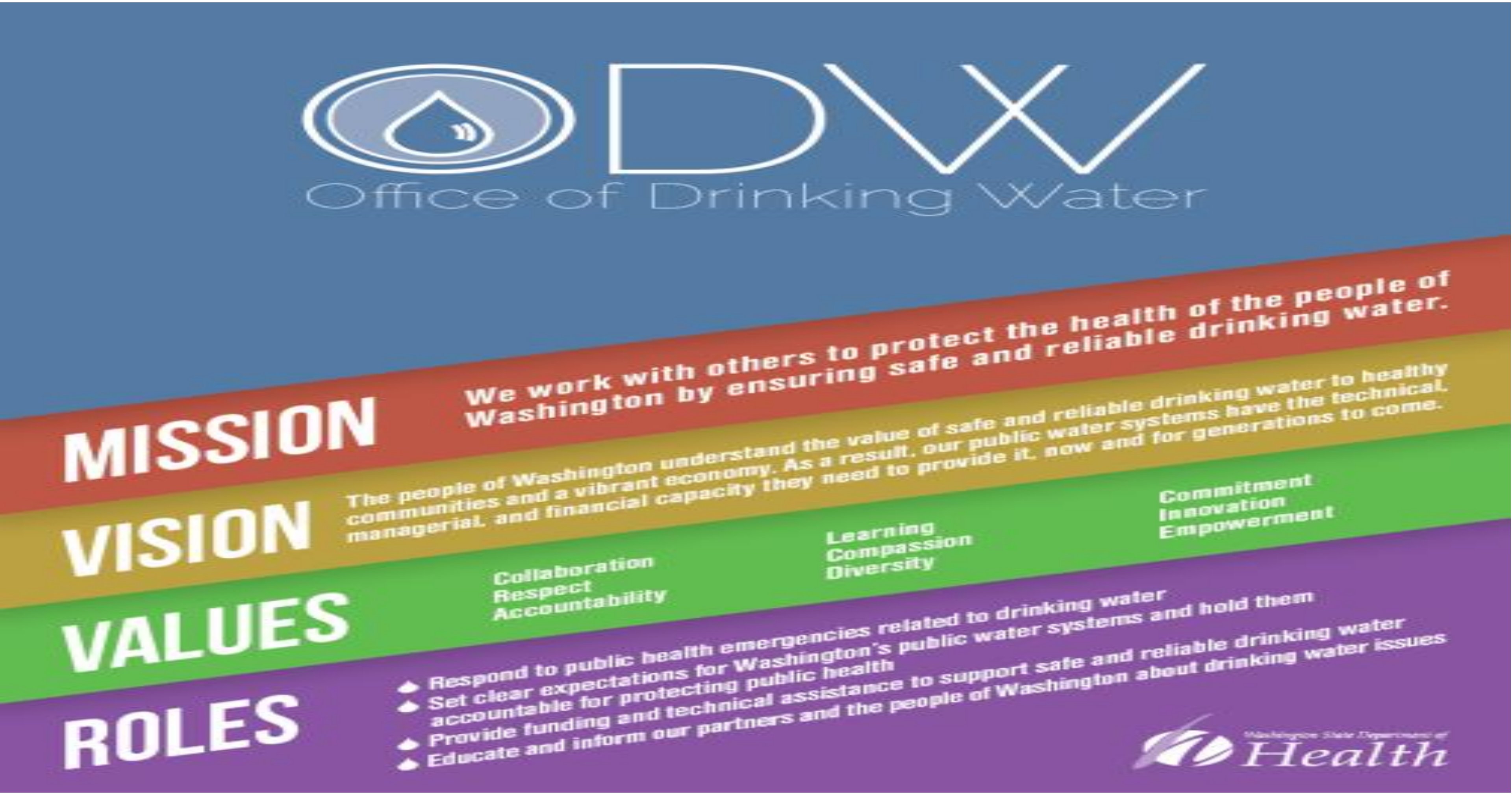
Washington State Department of HEALTH

WASHINGTON STATE CYBERESECURITY UPDATES

Office of Drinking Water



ODW

Office of Drinking Water

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

Washington State Department of Health

Importance of Cybersecurity

- Cyber attacks could negatively impact public health

- Cyber attacks could cause service disruptions

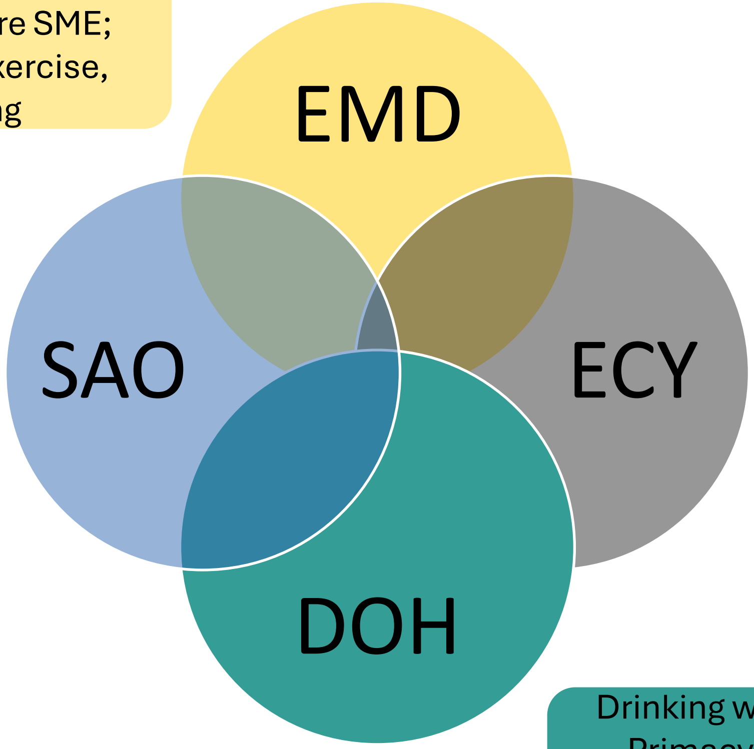
- Cyber attacks could cause disclosure of employee or customer personally identifiable information (PII)

- Cyber attacks could cause loss of public confidence and trust

Background for Cybersecurity Action Plan

- 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.

Collaborative Approach



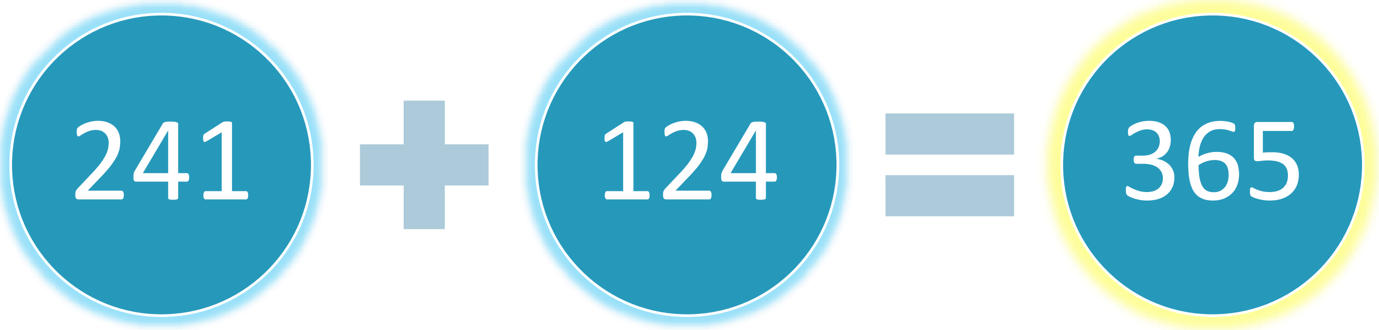
Cybersecurity & critical infrastructure SME; planning, exercise, training

Cybersecurity and critical infrastructure audits

Wastewater State Primacy Agency; outreach & engagement

Drinking water State Primacy Agency; outreach & engagement

Scope



241 + 124 = 365

<u>Drinking water systems:</u>

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

<u>Wastewater Treatment Plants:</u>

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

Total systems / facilities in scope

Cybersecurity Action Plan

Voluntary 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

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

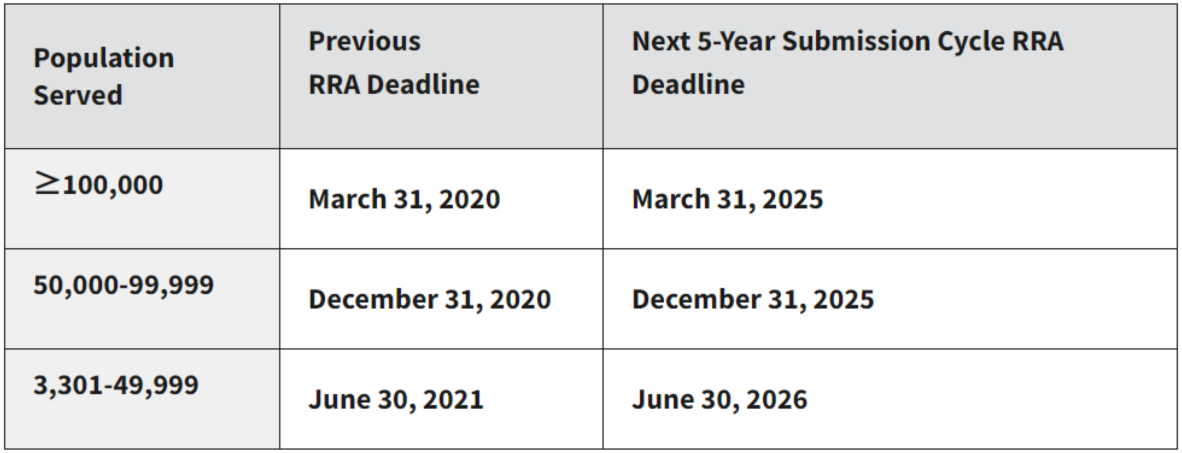
Emergency Response Plans (ERPs)

AWIA Requirements for Elements of ERPs:

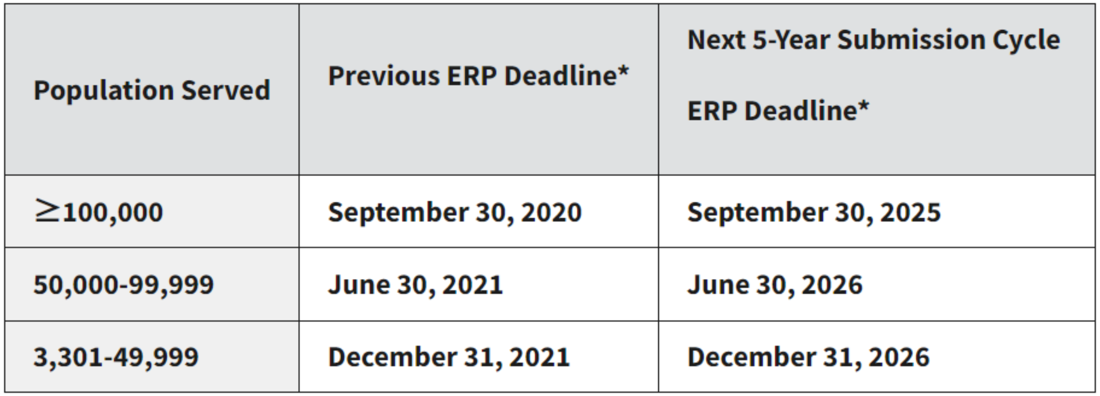
- Strategies to improve resilience, including physical and cyber security.
- Plans, procedures and equipment to be utilized in all hazards response.
- Actions, procedures, equipment to lessen impact on public health.
- Detection strategies

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

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

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. EPAs 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.

Point of Contact

Kim Moore

Policy Coordinator & Emergency Response Planner

Policy and Planning Section

Kimberly.Moore@doh.wa.gov

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

@WADeptHealth

Washington State Department of
HEALTH