

Emergency Preparedness



**CAN HELP
ENSURE
SAFE
DRINKING
WATER**

Oregon
Health
Authority

DRINKING WATER SERVICES
Public Health Division

Oregon
Health
Authority

Outline

- Emergency response plans (ERP)
- How to review ERPs during a survey
- Cybersecurity
- Workshops

What is an ERP?

- ◆ Procedures for routine and non-routine emergencies
- ◆ Reduces mistakes during emergencies and high stress situations
- ◆ Clear guidance for under-certified operators
 - ◆ Who assess the system's infrastructure?
 - ◆ Who handles repairs?
- ◆ Customer notification protocols
 - ◆ Who handles the media or questions from the public?
 - ◆ How to notify customers of advisories?

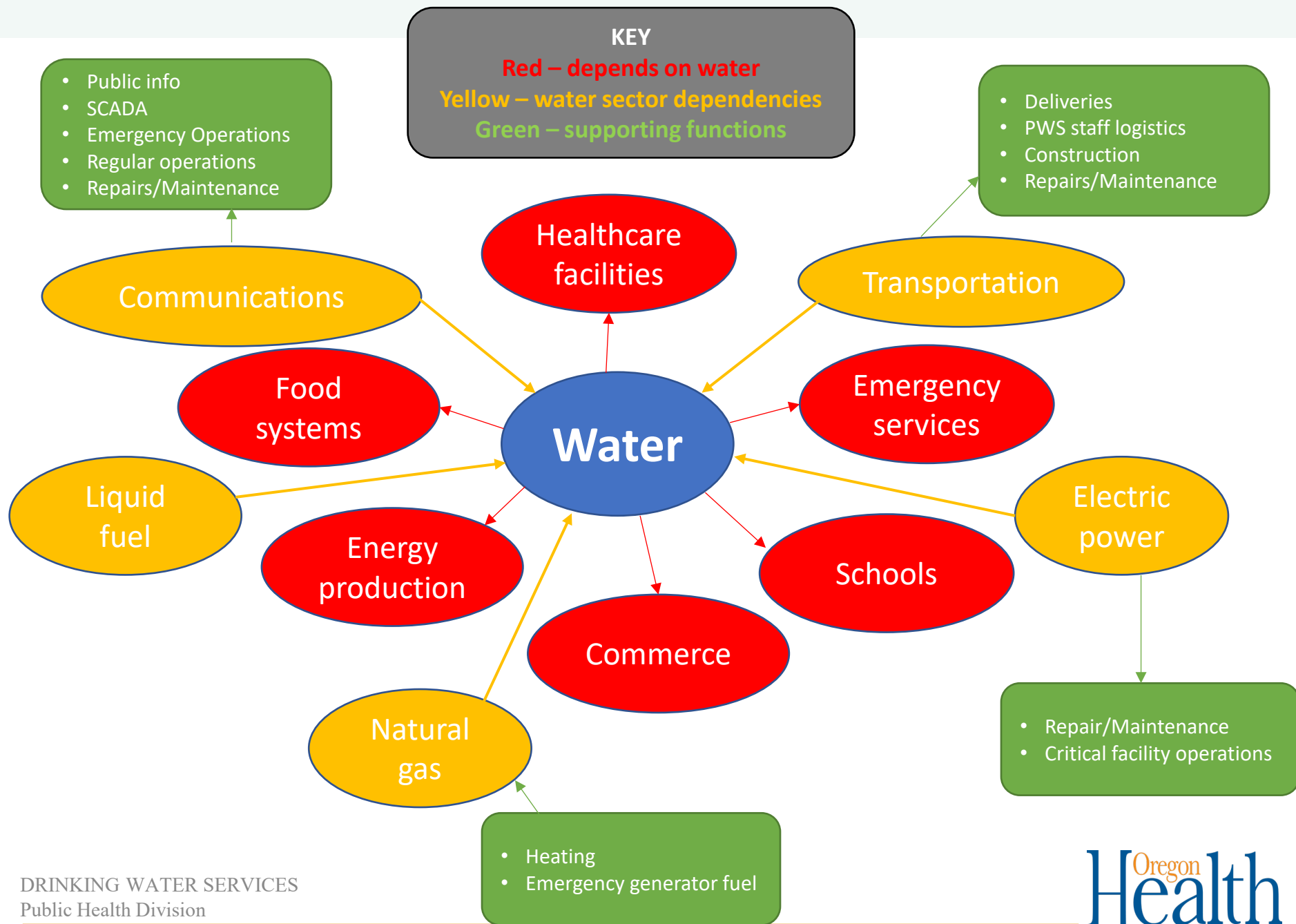


Why is it important?

ERPs can also help save money on response activities, resources, or equipment.

- Resource optimization – prioritize resources where they can make the biggest impact
- Business continuity
- Create community support (do this while developing the ERP)





Multiple Barrier Approach

No single barrier is perfect – multiple barriers can increase reliability of safe drinking water and decrease costs.

Q: What are the issues in the system, and what actions can we take to ensure safe drinking water?

- ◆ Source Water
- ◆ Operator certification
- ◆ Treatment
- ◆ Monitoring & reporting
- ◆ Water system surveys
- ◆ Operations (find & fix approach)
- ◆ Master plans
- ◆ Leak detection
- ◆ Public notification (consumer confidence reports, advisories, FAQs)
- ◆ O & M manuals
- ◆ ERPs

Oregon's ERP Requirements

CWS & NTNC systems serving 3,300 people or less

◆ Response procedures for:

- Isolating parts of the system,
- Emergency disinfection,
- Issuing boil or do-not-drink advisories,
- Loss of electrical power,
- Disruption/failure of disinfection or other treatment systems,
- Detection of E. coli bacteria or other contaminants exceeding the MCL,
- How to coordinate with local emergency managers, and
- Other reasonably anticipated emergencies.

Oregon's ERP Requirements

CWS & NTNC systems serving 3,300 people or less continued

- ◆ Plan for physical security
- ◆ Cybersecurity (if system utilizes computer networks, automated control, or monitoring process systems):
 - Establishing password policy based on current cybersecurity standards,
 - Creating a software update plan,
 - Monitoring for suspicious activity, and
 - Installing and updating anti-virus or anti-malware software.



American Water Works
Association

Oregon's ERP Requirements

All Oregon PWSs:

Certification: Systems do not need to send in or certify that their plans are complete.

Surveys: Ensure that ERPs are on hand for review.



It can be overwhelming, let's start small!

Identify

- Conduct asset inventory
- Risk & Resilience Assessment

Prepare

- Emergency Response Plan
- Water Conservation Plan

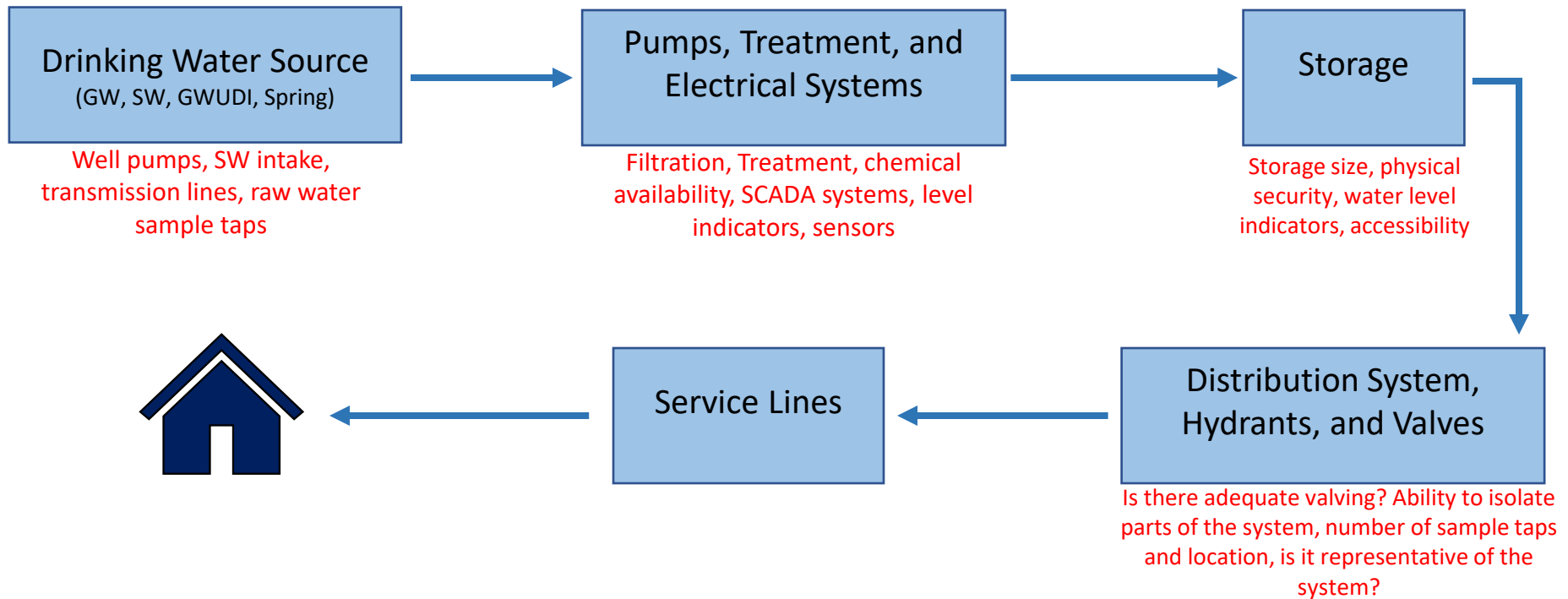
Implement

- Tabletop exercises
- Exercising the plan
- Work with local emergency managers

Identify

◆ Conduct an asset inventory

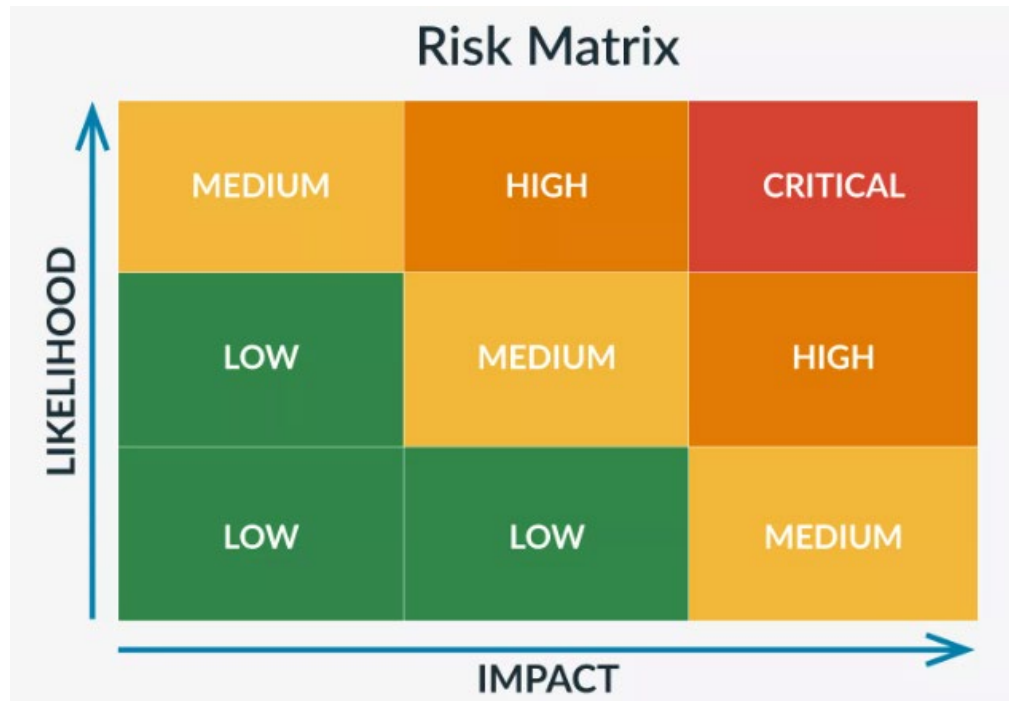
- ◆ What critical infrastructure or components does your system have?
- ◆ What are the technical, managerial, and operational functions needed to supply drinking water during an emergency?
- ◆ What is the life expectancy of the component?



Identify

♦ Risk & Resilience Assessment

- ♦ Based on your asset inventory, how would different emergencies impact system components and ability to supply drinking water?

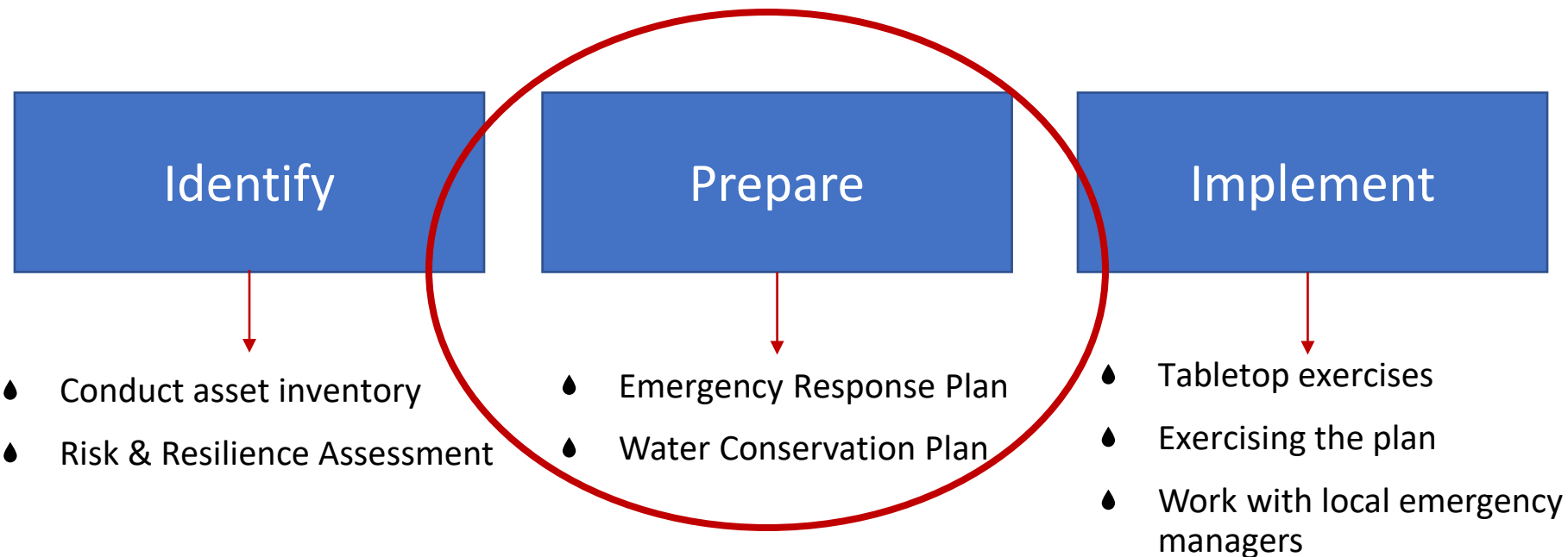


Identify

Examples

<u>Natural Hazards</u> <input type="checkbox"/> Flooding <input type="checkbox"/> Earthquake <input type="checkbox"/> Landslide <input type="checkbox"/> Windstorm <input type="checkbox"/> Ice/Snowstorm <input type="checkbox"/> Tsunami <input type="checkbox"/> Cyanotoxins/HABs <input type="checkbox"/> Wildfire <input type="checkbox"/> Drought <input type="checkbox"/> Other (list here)	<u>Critical Components at Risk to this Hazard</u> _____ _____ _____ _____ _____ _____ _____ _____ _____
<u>Man-Made Hazards or Malevolent Acts</u> <input type="checkbox"/> Physical attacks <input type="checkbox"/> Theft <input type="checkbox"/> Source water contamination <input type="checkbox"/> Intentional or accidental contamination of finished water <input type="checkbox"/> Cyberattack on process control or automated system <input type="checkbox"/> Cyberattack on financial infrastructure <input type="checkbox"/> Other (list here)	<u>Critical Components at Risk to this Hazard</u> _____ _____ _____ _____ _____ _____ _____

Area	Component/Asset	Importance	Risk	Priority	Notes
Source	SW Intake	High	High	High	high risk to wildfire, earthquake, flooding





ERP Considerations

- Have a limited budget?
 - Start small, think long term
 - Create a plan by prioritizing actions based on the risks and vulnerabilities found in the risk assessment
 - Involve water system management and the community
 - Work with other organizations



- Free technical assistance
- Develop plans
- Assist in building technical, managerial, and financial capacity





Circuit Rider Program

Services and Assistance

The Circuit Rider Program can support:

• Jar testing assistance	• Pump sizing
• Coagulant dosage optimization	• Cross-connection assistance
• Corrosion control implementation *	• Sampling plan assistance *
• Chemical feed math instruction	• Storage/distribution problems *
• Turbidimeter calibration	• Supply problems and water rights
• CT tracer studies *	• Research/investigation of alternatives
• Chemical feed pump calibration	• Recommendations for surface water treatment
• Filter troubleshooting *	• DBP reduction *
• Reporting and record keeping	• Filter media replacement
• Sampling requirements *	• Filter backwash rule compliance
• Valve adjustments	• Disinfection assistance *
• Minor changes to improve treatment and operation *	• Well repair/abandonment assistance
• Funding application assistance *	• Stage two monitoring requirements
• Financing options and strategies	

* Indicates common requests

Contact

Marlin Gochmour, PE, MBA - President
Civil West Engineering Services, Inc.
486 E Street

Coos Bay, OR 97420

Phone: 541-266-8601 | Fax: 541-266-8681 | Email: mgochnour@civilwest.net



ERP Considerations

Establish roles and responsibilities before emergencies

- Enhance communication and collaboration
- Improve accountability
- Streamline decision making

Chain of Command

(Review and update annually)

Staff name & title	Responsibilities during emergencies	Decision making authority	Emergency contact info

Where will the Emergency Response Plan be stored? _____

Have all personnel listed above been trained in the use of this plan? Yes ☐ No ☐

Would they all have access to the stored plan in an emergency? Yes ☐ No ☐

ERP Considerations

Staff preparedness and safety

- Plan for alternative communications
 - Staff emergency contact list
- Staff family safety (if family isn't safe, staff are less likely to be effective)
- Prepare emergency supplies in go-bags
 - food, water, medical, PPE, work equipment
- Plan for who is going to stay and work vs. who is not during an emergency
- Plan for safe alternative transportation routes
- Develop a buddy system



ERP Considerations

Water Hauling

- Unregulated
- Both haulers and PWS receiving hauled water should follow BMPs



BMPs

- Verify the source - use water from another PWS
- Use a food-grade tank or one dedicated for water
- Ensure proper inspection, cleaning, and disinfection of tank
- Measure free-chlorine residual upon arrival of the tank
- Ensure presence of an airgap to prevent backflow
- Boil water advisory
- See [DWS Water Hauling Guidelines](#)



ERP Considerations

Emergency water sources

Newly connected sources

- Sources not connected to the existing infrastructure must go through the plan review process and have approval before use
- If an emergency arises, contact the plan review team
 - Advisory may be needed

Temporary interties

- Connections with other nearby systems can help alleviate water supply issues
- Must go through plan review process and have approval

Existing emergency GW sources

- Before using – take steps to inspect the source, controls, treatment system, shock chlorinate, and flush.
- [Startup tips for GW wells](#)

ERP Considerations

Emergency Trailers

- Portable water treatment or distribution trailers in the event a PWS is unable to deliver water to distribution system
- Unregulated and does not require plan review
- Oregon Emergency Management (OEM) SPIRE Grant



BMPs

- Ensure proper filtration of surface water supplies
- Proper disinfection of the water
- All equipment coming into water is NSF Standard 61 or equivalent
- Consider issuing a boil water advisory for customers using water from these systems
- See [Emergency DW Facilities Guidelines](#)



Reporting Emergencies

Cybersecurity

- [CISA's cyber attack reporting form](#)
- CISA works with EPA and FBI to investigate and helps water systems respond to the attack

Any other emergency (water supply, drought, water hauling, wildfire impacts, flooding, etc.)

- Let your DWS contact person know the system's status and if resources are needed
 - Public notice advisories, infrastructure damage, different treatment, new sources, etc.
- Request assistance through local or county emergency manager
 - Bulk water distribution
- If the local or county emergency manager cannot fulfill, the request gets sent up to the state

Identify

- Conduct asset inventory
- Risk & Resilience Assessment

Prepare

- Emergency Response Plan
- Water Conservation Plan

Implement

- Tabletop exercises
- Exercising the plan
- Work with local emergency managers


How to review ERPs during a survey

- Emergency contact list (make sure contact info is up to date)
- Procedures:
 - How to isolate system
 - Emergency disinfection
 - Issuing public notices for customers
 - Loss of electrical power
 - Loss of distribution system pressure
 - Disruption/failure of disinfection or other treatment
 - Detection of E. coli bacteria or another contaminant exceeding the MCL
- Do they use SCADA or computer networks?
 - Password policy, software update plan, process for monitoring suspicious activity, installing/updating antivirus or anti-malware software

***Some procedures can be found in the O & M Manual**

How to review ERPs during a survey

Questions to ask yourself (and the operator) while reviewing the ERP:

- How often is the plan updated?
 - Is the plan easy to understand?
 - Has the system exercised the plan or any procedures?
 - Is it available for all staff during an emergency?
 - Is it dusty, or look like it hasn't been opened?
 - How does the system notify customers of an advisory?
 - Procedures for their reasonably anticipated emergencies?
- 
- Are procedures relevant to the system? A system that commonly goes through +TC detections should have a coliform sampling plan or response procedure

How to review ERPs

Significant deficiency vs. recommendation

- Is this the first significant deficiency for not having a complete ERP?
- Are there only a few items that need updating?
- Has the system corrected past significant deficiencies within a reasonable timeframe?
- Do you trust the operator to complete/update the ERP?

Use your best professional judgement!

Common recommendations:

- Ensure the emergency contact list, ERP procedures, or staff responsibilities are updated
- Include BMPs for mainline breaks, loss of pressure events
- Include procedures for emergency disinfection or shock chlorination



Windows

A fatal exception 0E has occurred at 0020:C0011E36 in UXD UMM(01) + 00010E36. The current application will be terminated.

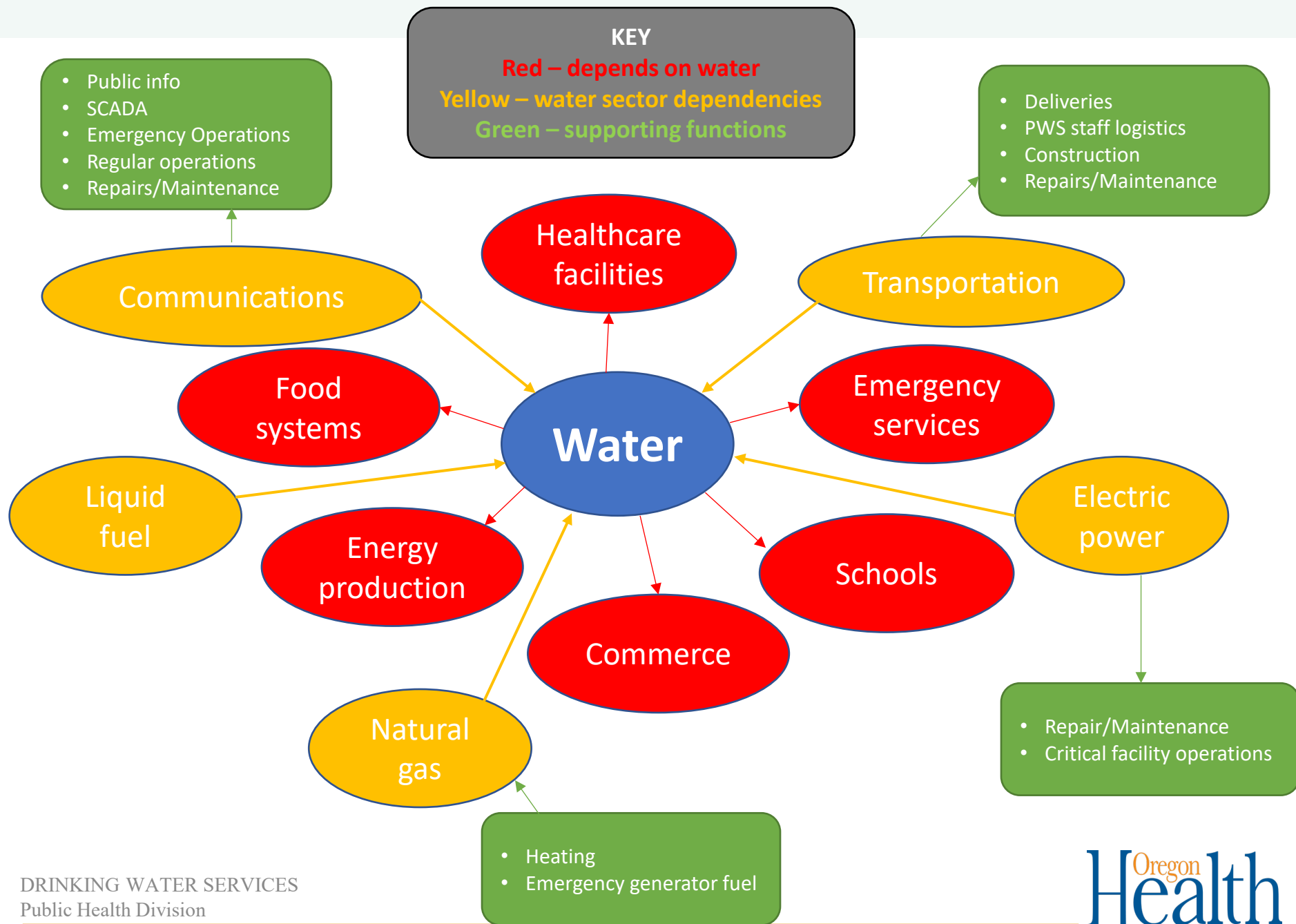
- * Press any key to terminate the current application.
- * Press CTRL+ALT+DEL again to restart your computer. You will lose any unsaved information in all applications.

Press any key to continue



Why are water systems attractive targets for cyber-attacks?

- Most PWSs are small and poorly secured.
 - Lack the resources and capacity to adopt rigorous cybersecurity practices.
- Water utilities are often overlooked compared to other critical infrastructure sectors such as power generation.
- Water system cyber-attacks can erode trust in institutions or organizations.
- Most critical infrastructure depend on water systems and potable water.
 - Hospitals, firefighting, emergency production



FEMA Community Lifelines



What can happen during a cyber-attack?

- Disruption of treatment or flow processes by opening/closing valves or disabling pumps
- Stealing customers' personal data or credit card info
- Defacement of utility website or electronic equipment
- Overriding alarms
- Access to critical locations
- Loss of monitoring processes
- Ransomware



Recent incidents focused on poorly protected small PWSs

- July 2023, Discovery Bay, CA – Servers running the WTP were disabled
- November 2023, Wylie, TX - Russian-affiliated Ransomware attack on PWS customers
- November 2023, Aliquippa, PA – Iranian attack on Unitronics PLC shut down booster pump station
- December 2023, Hawaii – PRC-backed ransomware attack on Hawaiian PWS
- December 2023, Multiple States - Iranian attacks on smaller water systems in multiple states
- January 2024, Muleshoe, TX – Russian hacking group caused water storage reservoir to overflow



Increase cyber resilience



- Restrict remote access
- Remove nonessential components, programs, or apps
- Change default passwords
- Restrict access and privileges for staff
- Ask ALL vendors about security practices
- Ability to switch to manual operations
- Backup OT/IT systems
- Train and test staff
- Cybersecurity assessments (free!)
- Develop an incident response and recovery plan

Cybersecurity Response

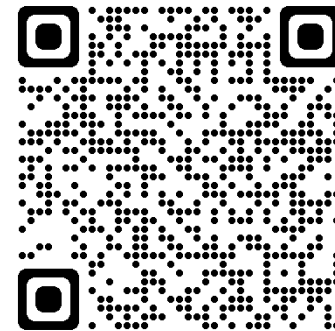
CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY



AMERICA'S CYBER DEFENSE AGENCY

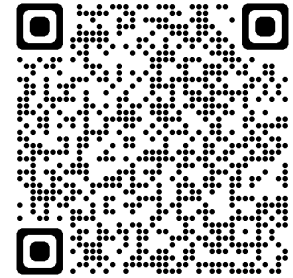


- ◆ Sign up for FREE cybersecurity risk assessments
 - ◆ CISA Region 10: Leslie Ann Kainoa, leslie.kainoa@cisa.dhs.gov, (503) 462-5626 (self assessment and in person)
 - ◆ [EPA's cybersecurity risk assessment](#) (self assessment and third-party)
- ◆ Report cybersecurity incidents
 - ◆ [CISA's cybersecurity incident reporting form](#)



State Cybersecurity Action Plan

March 28: White House sends letter to all state governors requesting a statewide cybersecurity action plan for water and wastewater systems due by June 28th.



- The plan must describe the state's approach to identify and address cybersecurity vulnerabilities for drinking water and wastewater systems.

Statewide Cybersecurity Action Plan Guidance:

- Decide which water/wastewater systems would be covered by plan (all water/wastewater systems, PWSs only, CWSs only, CWSs serving more than 3,300 people)
- Determine which systems have/have not completed cybersecurity assessments, mitigation plans or cyber incident response plans.
- Determine how the state will work with each system to establish a process for developing plans.

State Cybersecurity Action Plan

Draft: Oregon's statewide cybersecurity action plan includes all community water systems (and wastewater systems?) who utilize SCADA, IT, OT for monitoring and daily operations. The first step will include determining which systems are susceptible to cyber risks and have not completed a cybersecurity assessment. DWS will work with partnering agencies with cybersecurity expertise to contact each system to develop a cyber risk mitigation plan that includes vulnerabilities, specific actions to correct, and a schedule to exercise the plan. All stakeholders and agencies involved will need to ensure the cyber-risks and cybersecurity mitigation plans are exempt from public disclosure to protect critical infrastructure.

State Cybersecurity Action Plan

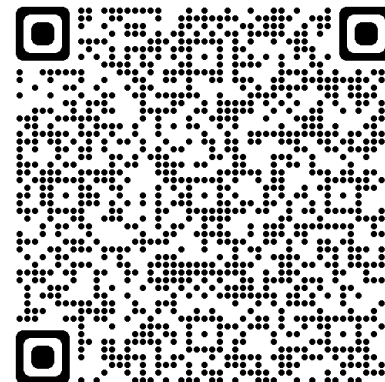


Next steps for Oregon:

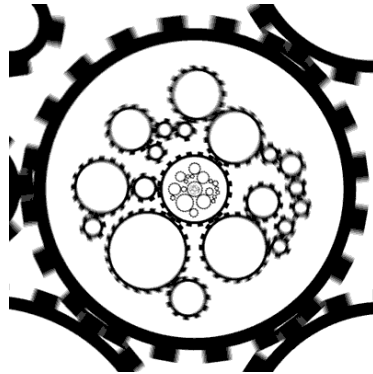
- Gather input from DWAC members
- Meet w/ DEQ to see if they will include wastewater systems in plan
- Meet with CISA Region 10 and Oregon Emergency Management to determine which agency will be in charge of outreach, conducting risk assessments, and assist in developing plans
- Determine which systems use SCADA/IT/OT
- Work with partner agencies to ensure risk assessments and mitigation plans are exempt from public disclosure rules

Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCI A)

- Proposed rulemaking published on April 4th establishes mandatory reporting for critical infrastructure sectors.
- Covered entities would be required to report cyber incidents to CISA within 72 hours, and 24 hours for a ransom payment.
- Reports would allow CISA to assist and provide resources to the impacted system.
- [Public comment due by June 3rd](#)
- More info: <https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia>



Switching gears... Workshops!



EPA/DWS Spill Response Workshop & Exercise

Draft Event Agenda: The following details a hypothetical draft, one day workshop agenda for discussion:

Day 1

Time (Pacific)	Topic	Facilitator
8:30 – 9:00 AM	Registration	Horsley Witten Group
9:00 – 9:15 AM	Welcome	Will Keefer, HW Parker Allen, EPA
9:15 – 9:30 AM	Spill Lessons Learned – either in Oregon or a national example	Parker Allen, EPA TBD, OHA
9:30 – 9:45 AM	Surface Water Emergency Response Plans/Geographic Response Plans	TBD, OHA TBD, EPA Region 10
9:45 – 10:00 AM	Surface Water Quantity and Quality Information and Tools	TBD
10:00 – 10:30 AM	EPCRA Tier II Reporting and America's Water Infrastructure Act (AWIA) Section 2018 Requirements (EPCRA Amendments)	Jeff Fencil, EPA TBD, OHA TBD, Local/County Agency
10:30 – 10:45 AM	Break	
10:45 – 11:00 AM	Spill Response – State & Federal Resources	TBD, OHA TBD, EPA Region 10
11:00 – 11:15 AM	Spill Response – Local Resources	TBD, Local/County Agency
11:15 – 11:30 AM	Water Supplier Perspective on Source Water Protection	TBD, Oregon Water Utility
11:30 – 11:45 AM	An Industry Perspective on Source Water Protection	TBD, Oregon Industry Partner
11:45 AM – 12:45 PM	Lunch	
12:45 – 1:00 PM	Tabletop Exercise Overview	Will Keefer, HW
1:00 – 2:30 PM	Tabletop Spill Exercise	Will Keefer, HW
2:30 – 2:45 PM	Break	
2:45 – 3:45 PM	Tabletop Exercise (continued)	Will Keefer, HW
3:45 – 4:00 PM	Closing Remarks and Evaluations	TBD
4:00 PM	Wrap-up & Adjourn	

- Location: In-person, Umpqua or Santiam basin
- Date: TBA – fall 2024
- EPA contractor will submit application for CEUs
- Discuss spill related preparedness and response activities
- Bring response agencies (state, county, local) with operators to discuss response plans, roles, and responsibilities

Any ideas for future emergency response or preparedness workshops?

Pop quiz time!



Are there cybersecurity requirements for Oregon PWSs?

A. Yes

B. No

Are there cybersecurity requirements for Oregon PWSs?

A. Yes!

CWS and NTNC systems serving 3,300 people or less: If water system utilizes computer networks or SCADA systems then cybersecurity measures must be implemented.

- Establishing password policy based on current cybersecurity standards
- Installing and regularly updating anti-virus or anti-malware software
- Monitoring for suspicious activity
- Creating a software update plan

CWS serving more than 3,300 people:

- Risk & resilience assessment must include the resilience and security of electronic, computer, or automated systems.
- Emergency response plan must include procedures that can reduce or eliminate the impact of malevolent, or man-made emergencies that can impact the supply of safe drinking water.
- Identify strategies that will aid in the detection of malevolent acts that threaten the security or resilience of the water system.

Who regulates emergency treatment and distribution trailers?

A. Drinking Water Services

B. These systems are not regulated

C. EPA

Who regulates emergency treatment and distribution trailers?

B. These systems are not regulated

What are BMPs when using water haulers/tankers?

- A. Use a food-grade tank or one dedicated for water**
- B. Ensure proper inspection, cleaning and disinfection**
- C. Use an airgap to prevent backflow**
- D. Issue a boil water advisory**
- E. All the above**

What are BMPs when using water haulers/tankers?

E. All the above

Do Oregon systems need to send in or certify to DWS that their ERPs are complete?

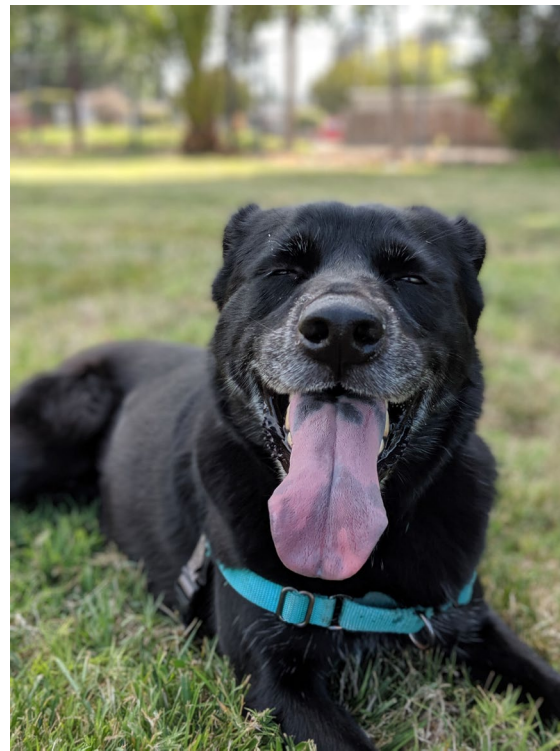
A. Yes

B. No

Do Oregon systems need to send in or certify to DWS that their ERPs are complete?

B. No

Thank you!



Chantal.t.Wikstrom@oha.Oregon.gov
971-666-8512