CYBER SECURITY SERVICES

Water and Wastewater Sector Cyber Guidance

Oregon's water and wastewater systems (herein referred to as "water systems") are part of the critical infrastructure that provides vital services to its citizens every day, however these same critical lifelines are also a target of cyber threats on a regular basis.

Water systems are targeted by malicious cyber groups and nation states alike, including those associated with the Iranian Revolutionary Guard Corps (IRGC) and the People's Republic of China (PRC) such as CyberAv3ngers[1] and Volt Typhoon[2], respectively. These malicious groups have targeted both Information Technology (IT) and Operational Technology (OT) systems, looking for any vulnerability that can be exploited to either make an immediate impact, or develop a foothold in the network for a targeted opportunity. Where any water system incident can result in a severe and damaging impact to the organization and the entire community, a continued dedication to cybersecurity best practices and planning are required and can establish an immediate improvement.

Cybersecurity best practices can scale from simple to in-depth, and some of the easiest changes can immediately defend against vulnerabilities recently exploited in attacks to water systems. Some best practices, resources, and contact information from both Enterprise Information Services (EIS) and our federal partners have been included.

Best Practices

Immediate & short-term	Medium- to long-term
Change default passwords immediately	Review/update plans & policies with best practices
Update software to address known vulnerabilities	Exercise plans to prepare, respond, and recover
Conduct cybersecurity awareness training	Inventory assets and backup systems

Initial Recommendations

Initial recommendations include the below and involve other actions to help protect vital services provided to Oregon:

- Communicate with your State & Federal cyber teams
- Reduce exposure to public-facing internet
- Conduct regular cybersecurity assessments
- Change default passwords immediately
- Conduct an inventory of OT/IT assets
- Develop and exercise cybersecurity incident response and recovery plans
- Backup OT/IT systems, immutable if possible
- Reduce exposure to vulnerabilities
- Conduct cybersecurity awareness training

1 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a
2 https://www.cisa.gov/news-events/news/us-and-international-partners-publish-cybersecurity-advisory-peoples-republic-china-state-sponsored

For more information scan the QR code or visit our website
security.oregon.gov

ENSURING ACCESSIBLE, RELIABLE, AND SECURE STATE TECHNOLOGY SYSTEMS THAT SERVE OREGONIANS.

Resources

Cybersecurity & Infrastructure Security Agency (CISA)

- Top Cyber Actions for Securing Water Systems | CISA
- Water and Wastewater Cybersecurity | CISA
- Critical Infrastructure Sectors page, that includes sector information and resources to include a sector-specific plan, working groups, and additional publications.
- Low- and no-cost services, including exercises, assessments, training, and more

Environmental Protection Agency (EPA)

- Drinking Water and Wastewater Resilience page
- Cybersecurity for the Water sector page which includes cybersecurity assessments, planning, training, response, and funding resources and information.
- Cybersecurity Technical Assistance Program that will support organizations in conducting an asset inventory.
- Cybersecurity Incident Action Checklist

Oregon EIS Cyber Security Services (CSS)

- Statewide guidance, policies, standards, and more can be found at our website https://security.oregon.gov.

Additional Resources

- Multi-State Information Sharing and Analysis Center (MS-ISAC)
- Water Information Sharing and Analysis Center (Water ISAC) is the only all-threats security information source for the water and wastewater sector

Incident contact Information

CISA

report@cisa.gov | 888-282-0870 | Report Site

EIS Security Operations Center (SOC)

Eso.soc@das.oregon.gov | 503-378-5930 | CSS Site

For more information scan the QR code or visit our website
security.oregon.gov

ENTERPRISE INFORMATION SERVICES
STATE CYBER COMMAND

ENSURING ACCESSIBLE, RELIABLE, AND SECURE STATE TECHNOLOGY SYSTEMS THAT SERVE OREGONIANS.