Meeting EPA Regulations to Protect Public Water Systems From Cyberattacks

Cyberattacks are a growing threat to critical infrastructure sectors, including water systems. Many critical infrastructure facilities have experienced cybersecurity incidents that led to the disruption of a business process or critical operation. Cyberattacks can compromise the ability of water utilities to provide safe water to customers, erode customer confidence, and result in financial and legal liabilities. A robust cybersecurity program can effectively reduce or even eliminate the vulnerabilities that cyberattacks exploit.

EPA Regulations for Public Water Systems

On March 3, 2023, the U.S. Environmental Protection Agency (EPA) issued regulations directing states to include cybersecurity when they conduct sanitation surveys, or audits, of public water systems (PWSs). EPA also released corresponding guidance that includes a checklist states can use to evaluate and improve the cybersecurity of their systems and meet these new requirements. If a significant deficiency in cybersecurity is identified by the sanitation survey, the state must notify the PWS, specify the corrective action it requires, and may provide deadlines for those actions.

Federal Funding is Available to Secure Water Systems

Funding is available for states and communities to meet cybersecurity threats through loans and set-asides provided through the Drinking Water State Revolving Fund. The EPA Fact Sheet expressly states, "EPA encourages states to utilize the significant increase in SRF funding for infrastructure projects that make water systems more resilient to all threats—whether it is natural disasters, climate change, or threats such as bioterrorism and cyberattacks." EPA also posted this SRF Cybersecurity Fact Sheet which details how the DWSRF may be used to support state programs and communities with cybersecurity measures.

Does your utility...

- ☐ Regularly review and maintain a list of all OT and IT assets with an IP address?
- ☐ Collect and store logs and/or network traffic data to detect cyberattacks and investigate suspicious activity?
- ☐ Maintain accurate documentation of the original and current configuration of OT and IT assets?
- ☐ Identify and patch vulnerabilities in a risk-informed manner (e.g., "critical assets first") as quickly as possible?
- ☐ Require strong passwords and password management practices?
- ☐ Deploy multi-factor authentication for IT and OT networks?
- ☐ Restrict System Administrator privileges to separate user accounts and evaluates administrative privileges on a recurring basis?
- ☐ Eliminate OT asset connections to the public Internet unless explicitly required for operations?

Source

EPA Office of Water. Evaluating Cybersecurity During Public Water System Sanitary Surveys. March 2023

Tenable OT Security Enables Public Water Systems to Identify and Prioritize Cyber Vulnerabilities

Tenable is the market leader in OT security and the only vendor that unifies exposure management for the modern attack surface. Security and compliance for critical infrastructure begins by getting an inventory of IT and OT assets on the network. Once there's a complete picture of the assets and how they are interconnected, Tenable Vulnerability Priority Rating (VPR) scoring generates vulnerability and risk levels using intelligence gained for each asset on the OT network. Reports include detailed insights, along with mitigation suggestions. This enables authorized personnel to quickly identify the highest risk for priority remediation before attackers can exploit vulnerabilities.

How Tenable OT Security Maps to the EPA's Cybersecurity **Checklist for Public Water System Sanitary Survey**

CHECKLIST CATEGORY	TENABLE CAPABILITY
Account Security (1.1-1.7)	**1.1, 1.2, 1.4** Tenable audits operating system (OS) configuration to ensure the control is active and will identify incorrect configuration via reports.
Device Security (2.1-2.5)	**2.2** Tenable audits OS configuration to ensure the control is active and will identify incorrect configuration via reports. **2.3** Tenable provides enterprise visibility, asset discovery and mapping. **2.5** Tenable establishes baseline settings on all OT devices and tracks deviations from the baseline, identifying configuration changes.
Data Security (3.1-3.4)	**3.1** Tenable collects network traffic and creates logs for use in forensic investigations. **3.2** Tenable stores security logs within Tenable OT Security, and can forward logs securely to 3rd party data repositories such as a SIEM or SOAR.
Vulnerability Management (5.1-5.6)	**5.1** Tenable leverages domain expertise in industrial security for OT assets, and Nessus for IT assets. Tenable's VPR scoring generates vulnerability and risk levels using each asset in your ICS network. Reports include detailed insights, along with mitigation suggestions. This enables authorized personnel to quickly identify the highest risk for priority remediation. **5.4** Tenable maps open ports and services allowing remediation.
Response and Recovery (7.1-7.4)	**7.4** Tenable maps the network and baselines its communications between all discovered devices aiding in the Incident Response (IR) process.

About Tenable

Tenable® is the Exposure Management company. More than 40,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies. Learn more at www.tenable.com.

For More Information: Please visit Tenable OT Security

Contact Us: Please email us at sales@tenable.com or visit tenable.com/contact