VFC WATER & WASTEWATER SECTOR ENGAGEMENT GUIDE

Cybersecurity Guidance and Resources for Water and Wastewater Sector Partners

The Water and Wastewater Sector (WWS) Engagement Guide provides sector partners with guidance on recommended actions to improve cybersecurity and reduce risk based on intelligence collected and activities observed by the Virginia Fusion Center (VFC). The guide also delivers a list of state, federal, and sector-specific resources available to address cyber threats to WWS organizations.

VFC WATER & WASTEWATER SECTOR ENGAGEMENT GUIDE

Understanding the Cyber Threat to Water Systems

Water and wastewater systems ("water systems") provide a necessary community lifeline that stretches across multiple critical infrastructure sectors. These systems face a range of cybersecurity threats due to their integration with modern digital technologies designed to improve operational efficiency and management. The increasing reliance on Supervisory Control and Data Acquisition (SCADA) systems, remote monitoring, and automated processes using Programable Logic Controllers (PLC's) has expanded the attack surface, making water systems unique targets for malicious cyber actors. Risks and threats can manifest in various forms including ransomware, zero-day exploits, or targeted nation-state activities, each of which can compromise system integrity, disrupt services, or potentially create a public health crisis.

Malicious cyber actors may exploit vulnerabilities in water system networks or connected equipment to gain unauthorized access or disrupt operations. In some cases, adversaries could target operational technology (OT) components directly, manipulating control systems to alter water quality or disrupt water supply processes. The impact of such attacks can be severe, leading to the contamination of drinking water, environmental damage, or even significant financial losses.

Collaboration across local, state, federal, and industry partners is necessary to combat this evolving threat. Through the continued development of joint initiatives such as comprehensive risk assessments, coordinated incident response strategies, and the identification of critical resource needs, all partners can contribute to statewide efforts that help ensure a secure and resilient Commonwealth.

Reporting an Incident in Virginia

The Virginia Fusion Center (VFC) acts as the primary point of contact for cyber incident reports in Virginia. Based on the severity and potential impact, partners from multiple agencies are activated to provide support for the impacted entity, with a focus on supporting the return to "*steady state*" as quickly and safely as possible.

Major cyber incidents, those which pose a threat to public health or safety, or community lifelines, also receive assistance from relevant emergency management partners in the Commonwealth.

Incidents can be reported to the VFC using the below:
vfc@vfc.vsp.virginia.gov;
reportcyber.virginia.gov;
804-674-2196.

USING THE VFC WWS ENGAGEMENT GUIDE

This guide was developed to address the growing threat malicious cyber actors pose to WWS entities in the Commonwealth of Virginia. It is not intended to replace any existing guidance or recommendations provided by federal, state, local, regional, sector-specific organizations, or regulatory entities. Rather, this document serves to offer additional guidance in applying a threat-based approach to cybersecurity risks in the Water and Wastewater Sector, based on intelligence collected and activities observed by the Virginia Fusion Center (VFC).

By using a threat-based approach, this guide breaks down core cybersecurity guidance into three sections - **People, Processes,** and **Technologies**. The VFC recognizes that these three sections and subsequent guidance are not all-encompassing of every action WWS organizations should take. Rather, the guidance provided here should be treated as additional considerations for partners to review, discuss, or implement as part of establishing a true defense-in-depth strategy.

Figure 1 - Core Sections of the VFC WWS Engagement Guide; People, Process, & Technology

To most effectively use this document, water system personnel should consider taking the following steps when beginning to review this guide:

1. **Identify or know the people/partners who play a critical role in the cybersecurity of your water system.**
2. **Collect and have available your existing policies, plans, and procedures relating to cybersecurity for quick reference.**
3. **Establish familiarity with the security technologies and/or frameworks currently in place within your organization.**
4. **Consider how the recommendations or resources identified in this guide can interact with (rather than replace) existing capabilities already in place to create layers of defense or prevention.**
5. **Coordinate a group of stakeholders within your organization to review and discuss this guide together to ensure a diversity of thought and input.**

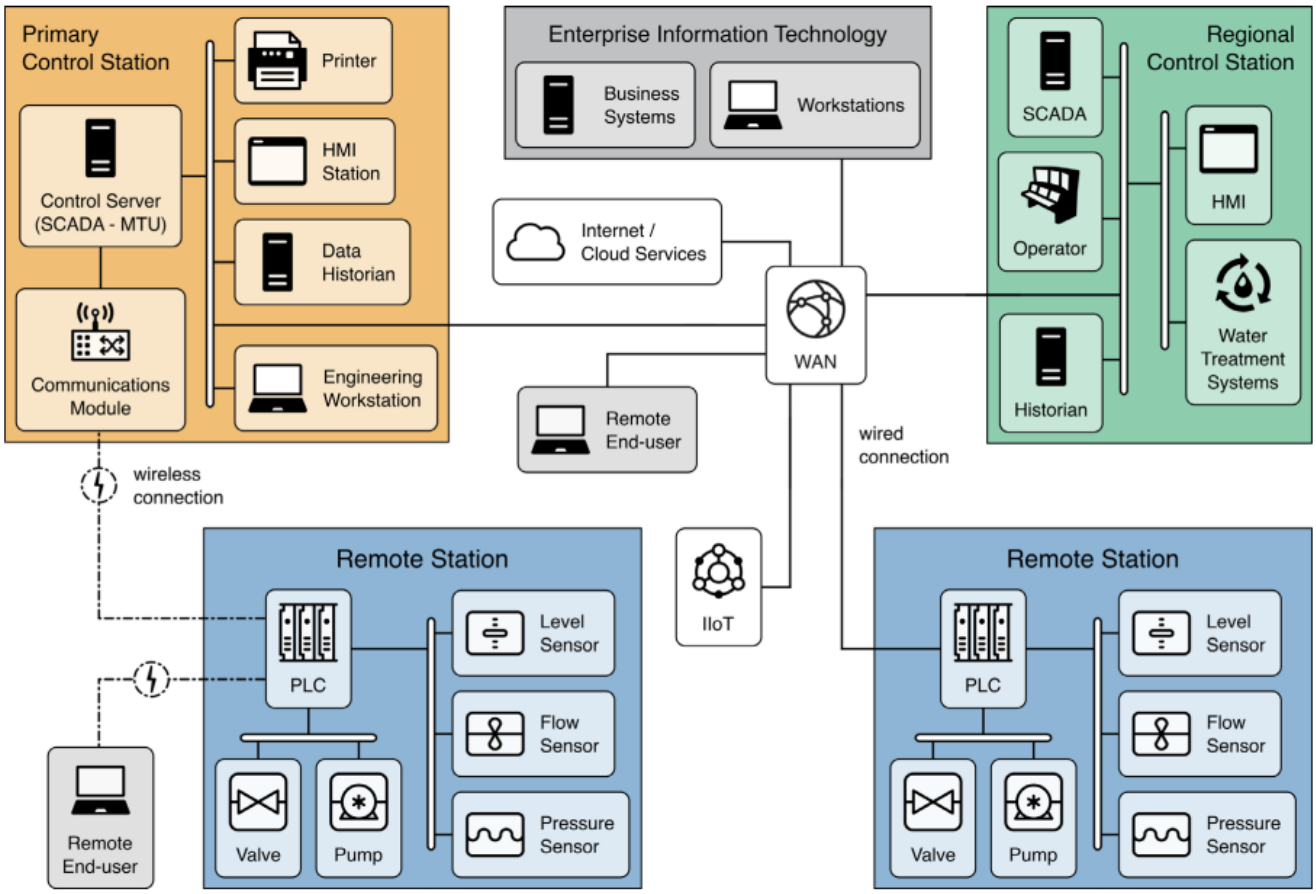

Figure 2. High-level architecture diagram of a fictional water system, courtesy of NIST.

UNDERSTANDING WATER SYSTEM NETWORKS

The above figure provides a simplified example of how a water system's information and operational technology architecture may look. This image helps to illustrate the complexity of these systems and the expanding attack surface that can develop. WWS entities may generally consist of some combination of the following components:

- A Primary and/or Regional Control Station which provides access to servers, historical data, SCADA systems, and treatment systems/sensors providing real-time control.
- Remote Stations which enable monitoring and management of field-based infrastructure such as pump stations and water distribution networks.
- Business Networks / Systems which provide office workers, business leaders, and support staff with routine network access relating to traditional business operations or organizational functions.
- Distributed PLC's and other industrial controls that enable water system operators to manage critical data relating to pressure, temperature, and chemical compositions.

CYBERSECURITY GUIDANCE FOR WWS

MITIGATING CYBER THREATS TO PEOPLE

- ☐ Establish enterprise and role-specific cybersecurity awareness training. Pursue technical and security training for operators.
  - EPA Cybersecurity 101 and 102 training
  - FEMA Critical Infrastructure Security and Resilience Courses
  - Virginia DEQ Wastewater Operator Training
  - Idaho National Laboratory ICS Cybersecurity Training
  - Request custom cybersecurity training from the VFC
- ☐ Implement security services to detect and block suspicious or malicious emails and phishing attacks targeting end-users.
  - CISA Managed List of Free Non-CISA Cybersecurity Services & Tools
- ☐ Block users from visiting known malicious web destinations.
  - MS-ISAC Malicious Domain Blocking & Reporting (public bodies only)
  - CISA Automated Indicator Sharing (AIS) Service
- ☐ Use geo-blocking to restrict access to unnecessary foreign websites and services.
- ☐ Enforce strong rotating passwords and/or password managers.
  - CISA Guidance on Choosing and Protecting Passwords
- ☐ Enforce multi-factor authentication, particularly on accounts used for remote access or virtual private networks (VPN's).
  - CISA More Than a Password Campaign
- ☐ Conduct exercises at least annually with a variety of stakeholders.
  - Virginia Department of Emergency Management Exercise Request
  - EPA Tabletop Exercise Tool
  - EPA Analytical Preparedness Full-Scale Exercise Toolkit
- ☐ Limit remote access to secure methods and only in those instances necessary for the organization. Restrict access to only trusted hosts when able. Maintain logs of all remote activities.
  - NIST Cybersecurity for WWS Build Architecture - OT Remote Access
- ☐ Maintain an up-to-date contact list and copies of critical plans with physical versions available. Update all plans at least annually.
- ☐ Subscribe to state, national, and sector-specific threat intelligence and information sharing service(s).
  - Virginia Fusion Center Intelligence Products Distribution List Signup
  - WaterISAC Membership Benefits
  - CISA Cybersecurity Alerts & Advisories
- ☐ Ensure the timely removal or account deactivation for users who have left the organization. Conduct routine audits of access/accounts.

Key Contacts

Virginia Fusion Center
804-674-2196
vfc@vfc.vsp.virginia
reportcyber.virginia.gov

VDH ODW
1-866-531-3068
Statewide Contact List

DEQ Wastewater
Wastewater Programs

VA Water Agency Response Network (VA WARN)
434-386-3190
vawarn.org

WaterISAC
1-866-426-4722
waterisac.org

EPA (Cyber Support)
888-282-0870
WICRD-outreach@epa.gov

DHS CISA
888-282-0870
central@cisa.dhs.gov
https://www.cisa.gov/water

Internet Crime Complaint Center (FBI)
804-261-1044
www.ic3.gov

What is Cyber Resilience?

Cyber resilience generally refers to an organization's ability to continuously deliver on its mission essential functions, or maintain its most critical business processes, even during a disruptive cyber attack.

This approach is different compared to traditional cybersecurity, which often focuses on prevention and protection. Instead, cyber resilience goals are focused on establishing the ability to **anticipate, withstand, recover, and adapt** to disruptive cyber incidents.

Cyber resilience can be achieved by enhancing your security practices through the inclusion of additional considerations around threat protection, risk management, and business continuity efforts.

BUILDING RESILIENT PROCESSES

- ☐ Establish a formal cybersecurity program within your organization.
  - EPA Water Sector Cybersecurity Brief for States
  - CISA Top Cyber Actions for Securing Water Systems
- ☐ Use a common security framework to ensure a structured approach in developing, baselining, and maturing your cyber program.
  - CISA Cross-Sector Cybersecurity Performance Goals
  - AWWA Water Sector Cybersecurity Risk Management Guidance for Small Systems
  - NIST Cyber Security Framework 2.0 Quick Start Guide
  - ISA/IEC 62443 Automation / Control System Cybersecurity Standards
- ☐ Develop and document a Cyber Incident Response Plan.
  - Request a copy of the VFC Cyber Incident Response Plan-in-a-Box
  - EPA Incident Action Checklist
  - CISA, FBI, and EPA Joint Incident Response Guide
- ☐ Ensure you have secure, off-site, and reliable backup solutions in place for critical IT and OT systems. Routinely validate these backups and conduct testing to verify systems can adequately restore from them when needed.
- ☐ Develop and document business continuity plans focused on the continuous delivery or rapid recovery of critical services during major incidents or outages.
  - FEMA Business Continuity Planning Suite
- ☐ Research opportunities to embrace organizational and community resilience as part of your security program.
  - NIST Community Resilience Planning Guide
  - Twice-weekly WaterISAC Security & Resilience Update (requires membership)
- ☐ Establish a vulnerability management process and prioritize patching.
  - CISA Cyber Vulnerability Scanning for Water Utilities
  - CISA Known Exploited Vulnerabilities Catalog
- ☐ Conduct cybersecurity and operational assessments at least annually.
  - VDH Water Infrastructure Security Resources & Tools
  - Request a Free Virginia National Guard Cyber Assessment through VDEM
  - EPA Cyber Assessments & Technical Assistance
  - CISA Risk and Vulnerability Assessments
  - Virginia DEQ Wastewater Onsite Assistance Program
- ☐ Join a Water and Wastewater Agency Response Network
  - Virginia Water and Wastewater Agency Response Network (VA WARN)
  - EPA Mutual Aid Assistance for Drinking Water and Wastewater Utilities
- ☐ Leverage the ICS4ICS framework for coordinated response.
  - Industrial Command System for Industrial Control Systems (ICS4ICS)

MANAGING CYBER THREATS TO TECHNOLOGY

- Embrace a defense-in-depth strategy to achieve a more robust security posture.
  - AWWA Water Sector Cybersecurity Risk Management Tool
  - DHS Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies
  - Critical Infrastructure Defense Project
- Establish an asset management program and/or asset inventory focused on discovery, identification, categorization, and management of all network-enabled devices and equipment.
  - VDH Capacity Development Guide: Asset Management
  - AWWA Resources for Asset Management
- Implement logging solutions to track activities on networks and/or end-points to aid in detection and response efforts.
  - CISA Logging Made Easy
- Reduce risks to public internet-facing infrastructure or services through removal or risk remediation efforts.
  - Request Information or to Join the VFC VAST Program
  - CISA Cyber Hygiene Services
  - CISA Stuff of Search Guide
- Validate that credentials are required for access on remote systems and no default usernames or passwords are still in use.
- Explore opportunities to implement zero trust architecture.
  - CISA Zero Trust Maturity Model
  - NSA Cybersecurity Information Sheet: Advancing Zero Trust Maturity Throughout the Network and Environment Pillar
- Learn more about INL's Cyber-Informed Engineering approach for building cybersecurity protections into critical infrastructure.
  - INL's Cyber-Informed Engineering Resources
- Utilize network segmentation practices with firewalls, data diodes, and software defined networks to minimize your risk if successfully compromised. Logically secure access to critically sensitive data or systems and apply role-based access controls.
  - NIST Cybersecurity for WWS: A Practical Reference Design for Mitigating Cyber Risk in Water & Wastewater Systems
  - PNNL Cyber Isolets System
- Apply appropriate encryption methods to protect data-at-rest and data-in-transit.
- Enable continuous monitoring solutions on the network through the use of intrusion detection and intrusion prevention systems.

More Training & Education Opportunities

SANS Training Purchase Discount - Through the SANS Water / Wastewater Utilities Partnership & the Aggregate Buy program, Public Water Utilities can get discounted training to improve their institution's security posture.

Resiliency for Water Utilities Program – This program from the Cyber Readiness Institute trains small and medium-sized water sector entities to become cyber ready.

TEEX Public Water System Security Course - This online course trains students on how to recognize and assess security issues related to water and wastewater plants.

Emergency Management for WWS Utilities – The EPA outlines core NIMS and ICS training recommended for WWS entities.

CISA ICS Training Calendar – Provides an up-to-date list of CISA-managed ICS trainings.

The National Cybersecurity Preparedness Consortium – The NCPC offers courses on numerous topics including ICS cyber resilience, network security, and zero trust architecture.