INCREASING CYBERSECURITY FOR WATER AND WASTEWATER UTILITIES

Lauren Wisniewski
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

Water and Wastewater Systems of All Sizes Are a Target

Why? Water and Wastewater Systems are Target Rich and Vital to Communities

- Typically, have limited cybersecurity resources
- Information Technology (IT)/Operational Technology (OT) convergence increases threat attack surface
- Most critical infrastructure (e.g., hospitals, firefighting, energy production) depends on water and wastewater systems

Who? Anyone, Anywhere

- Strong organized state actors attempting to disrupt our way of life
- Mid to low level criminals looking for a quick buck or make a political statement
- Insider threats from accidental everyday operations to disgruntle employees

Water and Wastewater Systems of All Sizes Are Impacted

What? Water and Wastewater Systems have experienced financial and operational impacts

- Disruption of treatment and conveyance processes by opening and closing valves, overriding alarms or disabling pumps or other equipment
- Defacement the utility's website or electronics equipment
- Stolen customers' personal data or credit card information
- Malicious programs like ransomware, which can disable business enterprise or process control operations
- Financial and legal liabilities

This photo provided by the Municipal Water Authority of Aliquippa shows the screen of a Unitronics device that was hacked in Aliquippa, Pennsylvania on November 25, 2023.
Municipal Water Authority of Aliquippa via AP

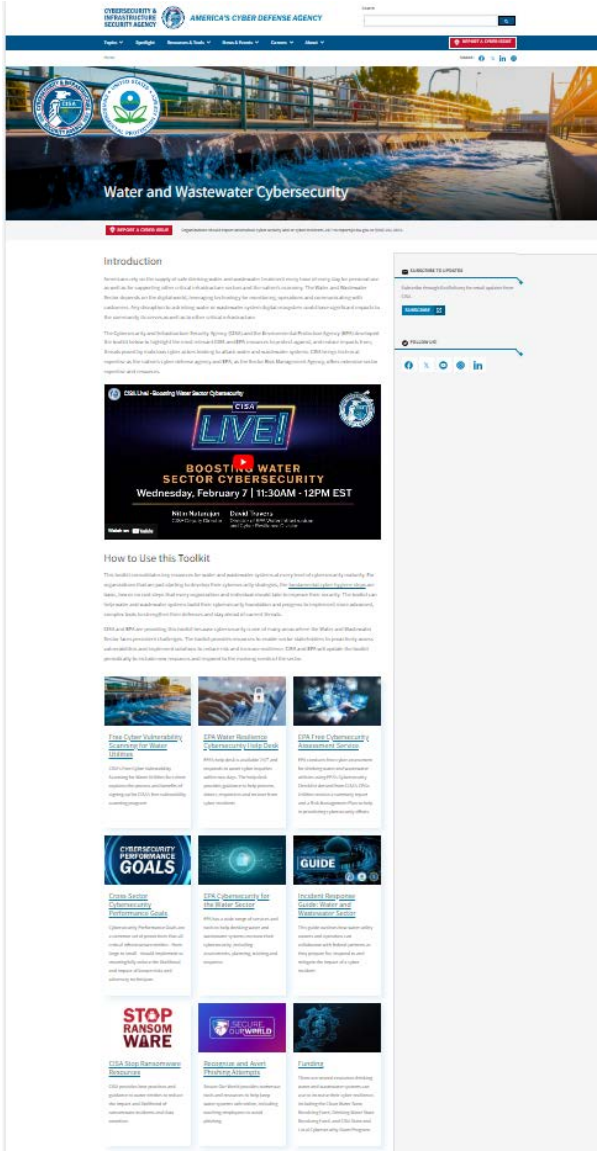
Cybersecurity is For Everyone

- Recognize and Report Phishing
- Use Strong Passwords
- Turn on Multifactor Authentication (MFA)
- Update Software

Lauren Wisniewski
April 3, 2024

CISA-EPA Water and Wastewater Toolkit

- Available at https://www.cisa.gov/water
- Consolidates most vital CISA and EPA information, resources, and tools for water and wastewater systems
- Resources include:
  - Free vulnerability scanning
  - Free cybersecurity assessments
  - Incident Response Guidance
  - Technical assistance support
  - Contact information for CISA Regions
  - Stop Ransomware resources



Free Cyber Vulnerability Scanning

Purpose: Assess Internet-accessible systems for known vulnerabilities and configuration errors.

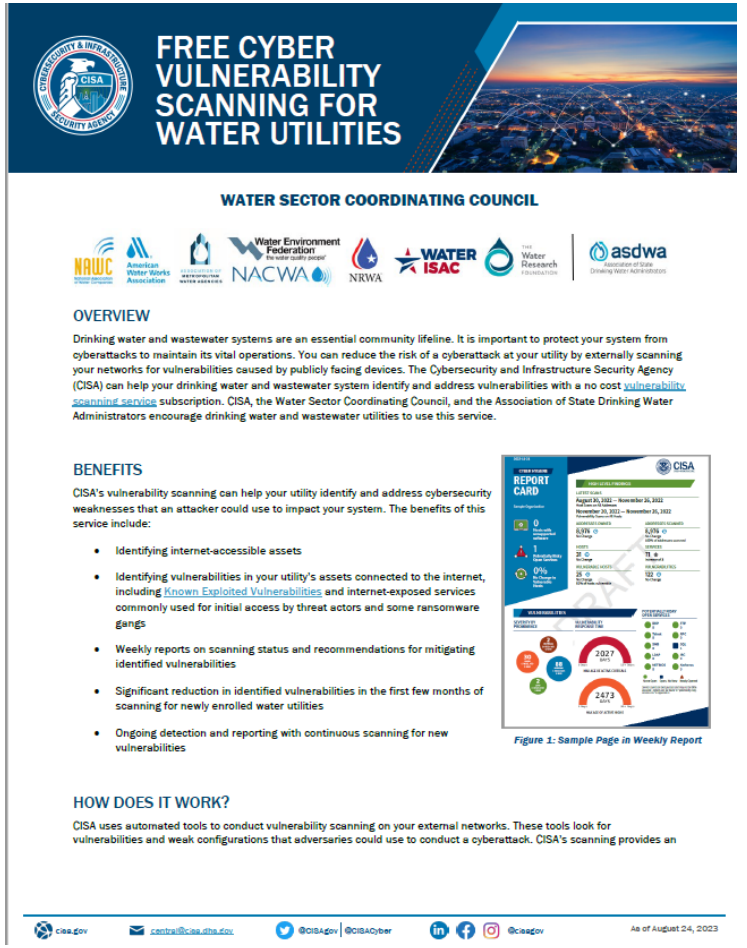
Delivery: Identify public-facing Internet security risks, through service enumeration and vulnerability scanning online by CISA.

Benefits:

- Continual review of system to identify potential problems
- Weekly reports detailing current and previously mitigated vulnerabilities
- Recommended mitigation for identified vulnerabilities

Network Vulnerability & Configuration Scanning:

- Identify network vulnerabilities and weakness



FREE CYBER VULNERABILITY SCANNING FOR WATER UTILITIES

WATER SECTOR COORDINATING COUNCIL

OVERVIEW

Drinking water and wastewater systems are an essential community lifeline. It is important to protect your system from cyberattacks to maintain its vital operations. You can reduce the risk of a cyberattack at your utility by externally scanning your networks for vulnerabilities caused by publicly facing devices. The Cybersecurity and Infrastructure Security Agency (CISA) can help your drinking water and wastewater system identify and address vulnerabilities with a no cost vulnerability scanning service subscription. CISA, the Water Sector Coordinating Council, and the Association of State Drinking Water Administrators encourage drinking water and wastewater utilities to use this service.

BENEFITS

CISA's vulnerability scanning can help your utility identify and address cybersecurity weaknesses that an attacker could use to impact your system. The benefits of this service include:

- Identifying internet-accessible assets
- Identifying vulnerabilities in your utility's assets connected to the internet, including Known Exploited Vulnerabilities and internet-exposed services commonly used for initial access by threat actors and some ransomware gangs
- Weekly reports on scanning status and recommendations for mitigating identified vulnerabilities
- Significant reduction in identified vulnerabilities in the first few months of scanning for newly enrolled water utilities
- Ongoing detection and reporting with continuous scanning for new vulnerabilities

Figure 1: Sample Page in Weekly Report

HOW DOES IT WORK?

CISA uses automated tools to conduct vulnerability scanning on your external networks. These tools look for vulnerabilities and weak configurations that adversaries could use to conduct a cyberattack. CISA's scanning provides an

As of August 24, 2023

Benefits of Vulnerability Scanning

Known exploited vulnerabilities are easy access for attackers, with **incidents averaging $100,000 in damages** for small and medium businesses.

CISA's free vulnerability scanning service helps **identify exposed assets and exploitable vulnerabilities** and is proven to reduce risk for participating organizations.

Avoid costly disruptions with early detection and action. Through weekly reports and timely alerts, we will help you **act before others take advantage**.

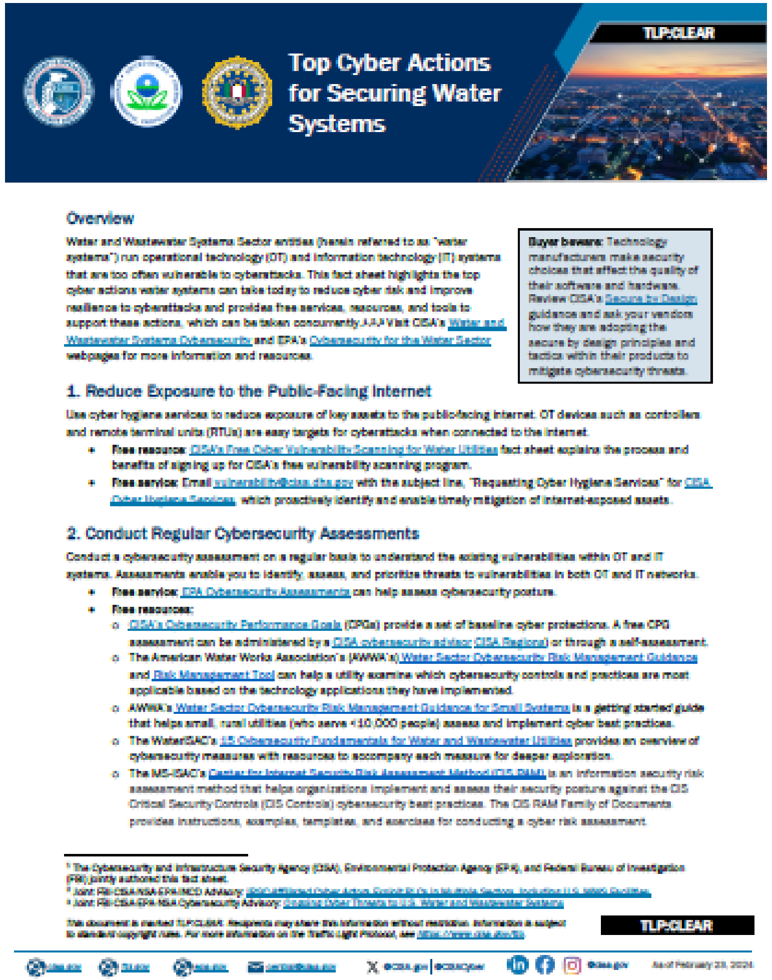
BY THE NUMBERS

- **7,200+** current customers nationwide
- **Over 3 Million** vulnerabilities found and fixed
- On average a **40% reduction in risk and exposure** by newly enrolled customers in their first 12 months
- Most enrollees see improvements within the first **90 days**

Lauren Wisniewski
April 3, 2024

Top Cyber Actions for Securing Water Systems

1. Reduce Exposure to the Public-Facing Internet
2. Conduct Regular Cybersecurity Assessments
3. Change Default Passwords Immediately
4. Conduct an Inventory of Operational Technology/Information Technology Assets
5. Develop and Exercise Cybersecurity Incident Response and Recovery Plans
6. Backup OT/IT Systems
7. Reduce Exposure to Vulnerabilities
8. Conduct Cybersecurity Awareness Training



TLP:CLEAR

Top Cyber Actions for Securing Water Systems

Overview

Water and Wastewater Systems Sector entities (herein referred to as "water systems") run operational technology (OT) and information technology (IT) systems that are too often vulnerable to cyberattacks. This fact sheet highlights the top cyber actions water systems can take today to reduce cyber risk and improve resilience to cyberattacks and provides free services, resources, and tools to support these actions, which can be taken concurrently.[1,2,3] Visit CISA's Water and Wastewater Systems Cybersecurity and EPA's Cybersecurity for the Water Sector webpages for more information and resources.

Buyer beware: Technology manufacturers make security choices that affect the quality of their software and hardware. Review CISA's Secure by Design guidance and ask your vendors how they are adopting the secure by design principles and tactics within their products to mitigate cybersecurity threats.

1. Reduce Exposure to the Public-Facing Internet

Use cyber hygiene services to reduce exposure of key assets to the public-facing internet. OT devices such as controllers and remote terminal units (RTUs) are easy targets for cyberattacks when connected to the internet.

- **Free resource:** CISA's Free Cyber Vulnerability Scanning for Water Utilities fact sheet explains the process and benefits of signing up for CISA's free vulnerability scanning program.
- **Free service:** Email vulnerability@cisa.dhs.gov with the subject line, "Requesting Cyber Hygiene Services" for CISA Cyber Hygiene Services, which proactively identify and enable timely mitigation of internet-exposed assets.

2. Conduct Regular Cybersecurity Assessments

Conduct a cybersecurity assessment on a regular basis to understand the existing vulnerabilities within OT and IT systems. Assessments enable you to identify, assess, and prioritize threats to vulnerabilities in both OT and IT networks.

- **Free service:** CISA Cybersecurity Assessments can help assess cybersecurity posture.
- **Free resources:**
  - CISA's Cybersecurity Performance Goals (CPGs) provide a set of baseline cyber protections. A free CPG assessment can be administered by a CISA cybersecurity advisor (CISA Regions) or through a self-assessment.
  - The American Water Works Association's (AWWA's) Water Sector Cybersecurity Risk Management Guidance and Risk Management Tool can help a utility examine which cybersecurity controls and practices are most applicable based on the technology applications they have implemented.
  - AWWA's Water Sector Cybersecurity Risk Management Guidance for Small Systems is a getting started guide that helps small, rural utilities (who serve <10,000 people) assess and implement cyber best practices.
  - The WaterISAC's 15 Cybersecurity Fundamentals for Water and Wastewater Utilities provides an overview of cybersecurity measures with resources to accompany each measure for deeper exploration.
  - The MS-ISAC's Center for Internet Security Risk Assessment Method (CIS RAM) is an information security risk assessment method that helps organizations implement and assess their security posture against the CIS Critical Security Controls (CIS Controls) cybersecurity best practices. The CIS RAM Family of Documents provides instructions, examples, templates, and exercises for conducting a cyber risk assessment.

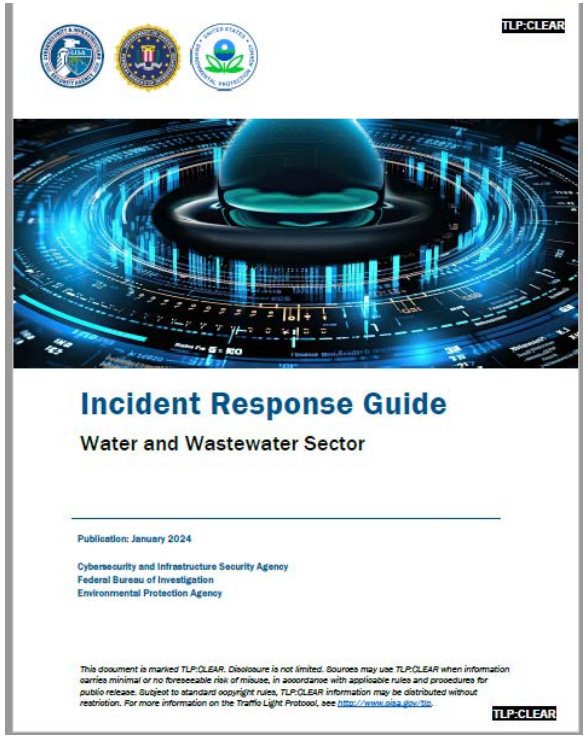
[1] The Cybersecurity and Infrastructure Security Agency (CISA), Environmental Protection Agency (EPA), and Federal Bureau of Investigation (FBI) jointly authored this fact sheet.

TLP:CLEAR

Lauren Wisniewski
April 3, 2024

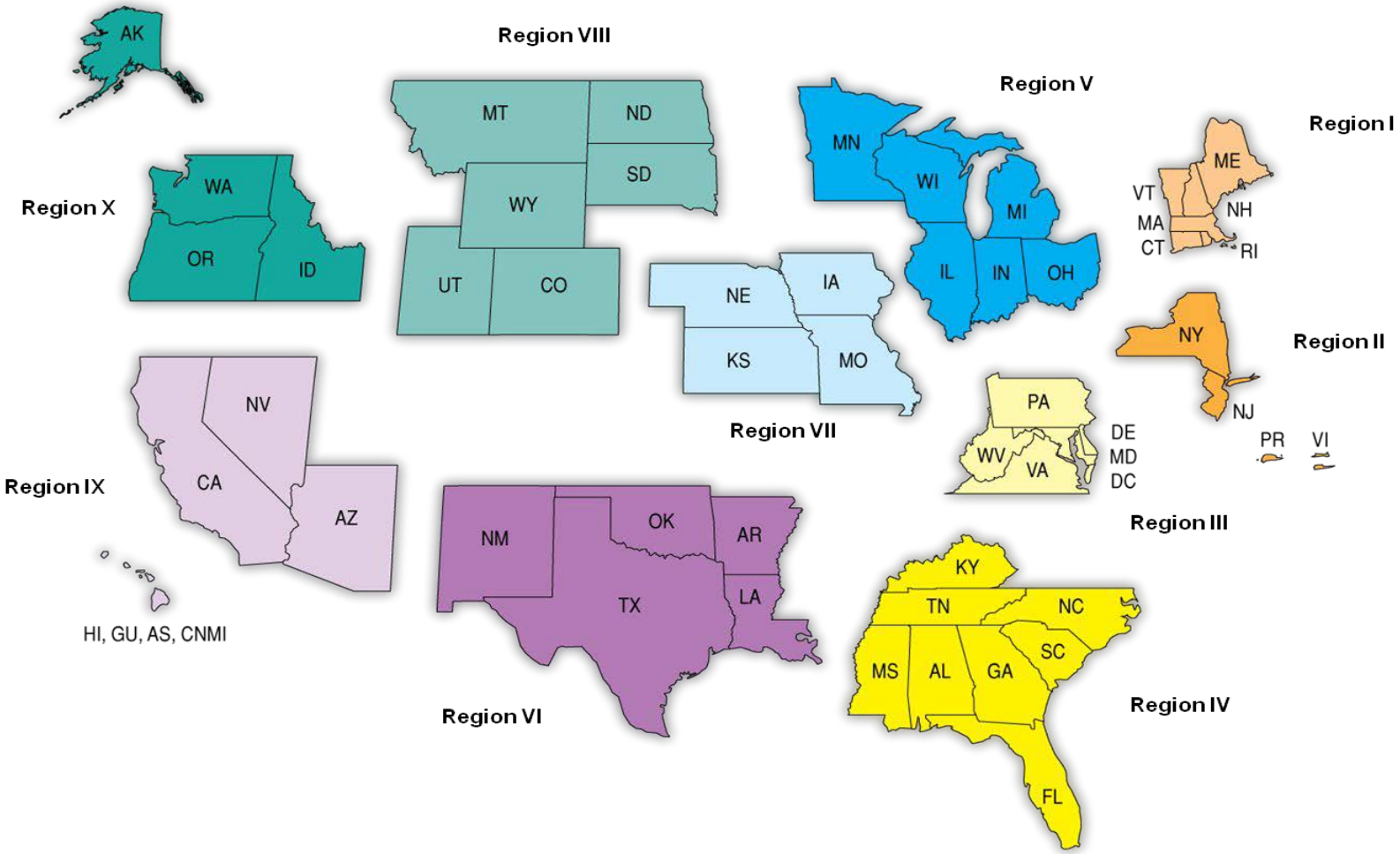
Responding to and Reporting Cyber Incidents

- Incident Response Guide Water and Wastewater Sector outlines how water utility owners and operators can coordinate with federal partners as they:
  - prepare for,
  - respond to, and
  - mitigate the impact of a cyber incident.
- Cyber Incident Reporting for Critical Infrastructure Act
- Report Cyber Incidents
  - cisa.gov/report
  - Email: report@cisa.gov
  - Call 888-282-0870



Lauren Wisniewski
April 3, 2024

CISA Regional Staff



Regional Personnel:

- Cybersecurity Advisors (CSAs)
- Cybersecurity Coordinators
- Protective Security Advisors (PSAs)
- Emergency Communications Coordinators
- Chemical Security Inspectors

Lauren Wisniewski
April 3, 2024

State and Local Cybersecurity Grant Program (SLCGP)

- GOAL: help states, local governments, rural areas, tribes, and territories address cybersecurity risks and cybersecurity threats to information systems.
- OBJECTIVES:
  1. Implement cyber governance and planning
  2. Assess and evaluate systems and capabilities
  3. Mitigate prioritized issues
  4. Build a cybersecurity workforce

- Fiscal Year (FY) 2022 focused on Objective 1, while FY 2023 focuses on Objectives 2 and 3.

Thank You

Contact Information

Lauren Wisniewski
Cybersecurity and Infrastructure Security Agency
Water and Wastewater Sector Liaison
lauren.wisniewski@cisa.dhs.gov