CYBERSECURITY FOR WATER AND WASTEWATER SYSTEMS

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

CISA Mission and Vision

MISSION:

We lead the National effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

VISION:

Secure and resilient infrastructure for the American people.

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, Anybody**
  - 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

Common Goals for Cyber Criminals: Water and Wastewater Systems

- Disrupt treatment and conveyance processes by opening and closing valves, overriding alarms or disabling pumps or other equipment

- Deface the utility's website or compromise the email system

- Steal customers' personal data or credit card information from the utility's billing system

- Install malicious programs like ransomware, which can disable business enterprise or process control operations

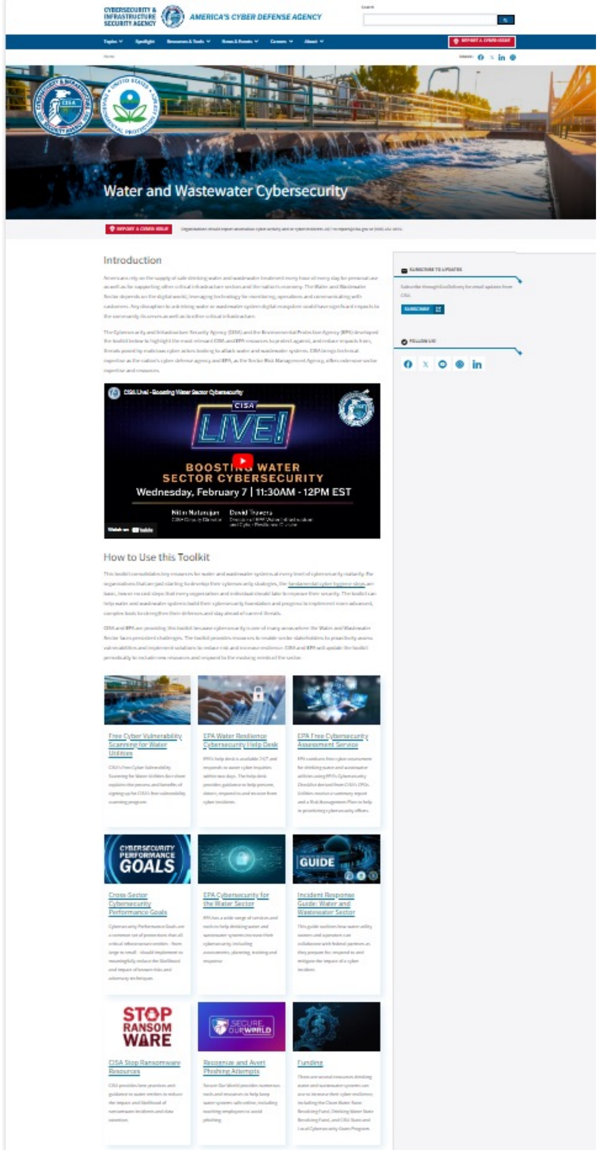
- Compromise the ability of water and wastewater utilities to provide clean and safe water to customers, erode customer confidence, and result in financial and legal liabilities

Cyber Av3ngers Threat Activity - Water and Wastewater Sector

- Since at least November 22, 2023, Iranian Government Islamic Revolutionary Guard Corps (IRGC)-affiliated cyber actors using the persona "CyberAv3ngers" have actively targeted and compromised Israeli-made Unitronics Vision Series programmable logic controllers (PLCs).
- Cyber actors left a defacement image stating, *"You have been hacked, down with Israel. Every equipment 'made in Israel' is CyberAv3ngers legal target."*
- Multiple water and wastewater systems across multiple states were impacted.
- Impacted PLCs and Human Machine Interfaces (HMIs) were deployed with Default Password – "1 1 1 1"

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



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

Water and Wastewater Cybersecurity

Introduction

[illegible]

CISA Live! - Boosting Water Sector Cybersecurity

BOOSTING WATER SECTOR CYBERSECURITY

Wednesday, February 7 | 11:30AM - 12PM EST

How to Use this Toolkit

[illegible]

Free Cyber Vulnerability Scanning for Water Utilities

EPA Water Resilience Cybersecurity Help Desk

EPA Free Cybersecurity Assessment Service

Cross-Sector Cybersecurity Performance Goals

EPA Cybersecurity for the Water Sector

Incident Response Guide: Water and Wastewater Sector

CISA Stop Ransomware Resources

Recognize and Avert Phishing Attempts

Funding

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

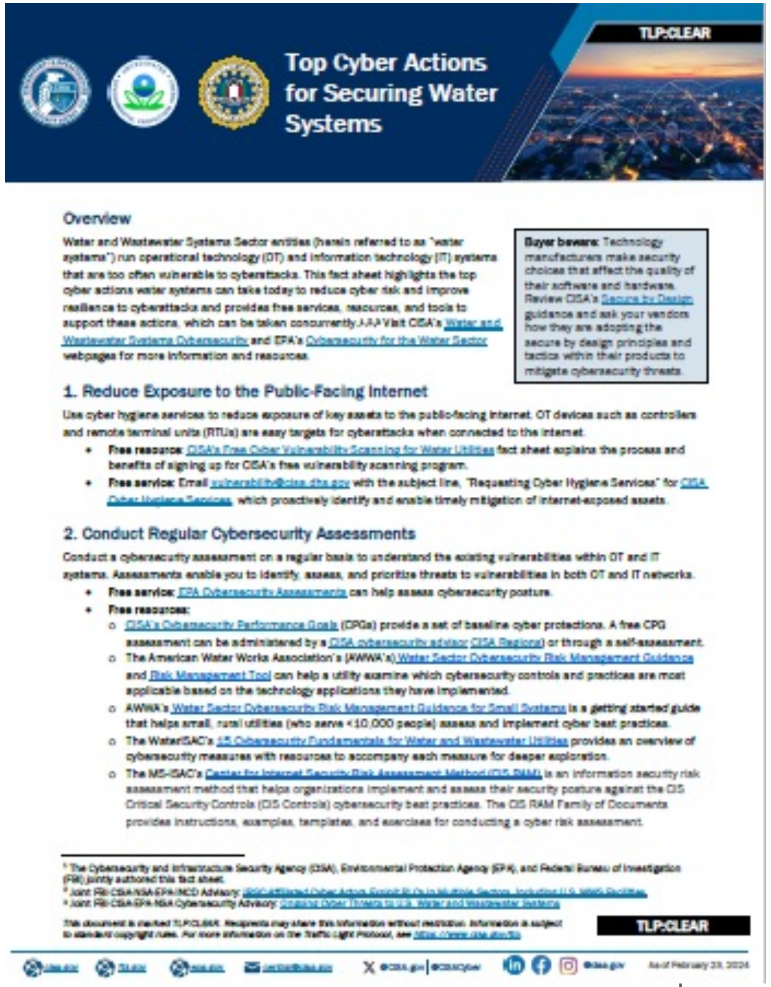
HOW DOES IT WORK?

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

cisa.gov central@cisa.dhs.gov @CISAgov | @CISACyber @cisagov As of August 24, 2023

Top Cyber Actions for Securing Water Systems

- Reduce Exposure to the Public-Facing Internet
- Conduct Regular Cybersecurity Assessments
- Change Default Passwords Immediately
- Conduct an Inventory of Operational Technology/Information Technology Assets
- Develop and Exercise Cybersecurity Incident Response and Recovery Plans
- Backup OT/IT Systems
- Reduce Exposure to Vulnerabilities
- 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:** EPA 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.

[2] Joint FBI-CISA-NSA-EPA-INCD Advisory: IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. WWS Facilities

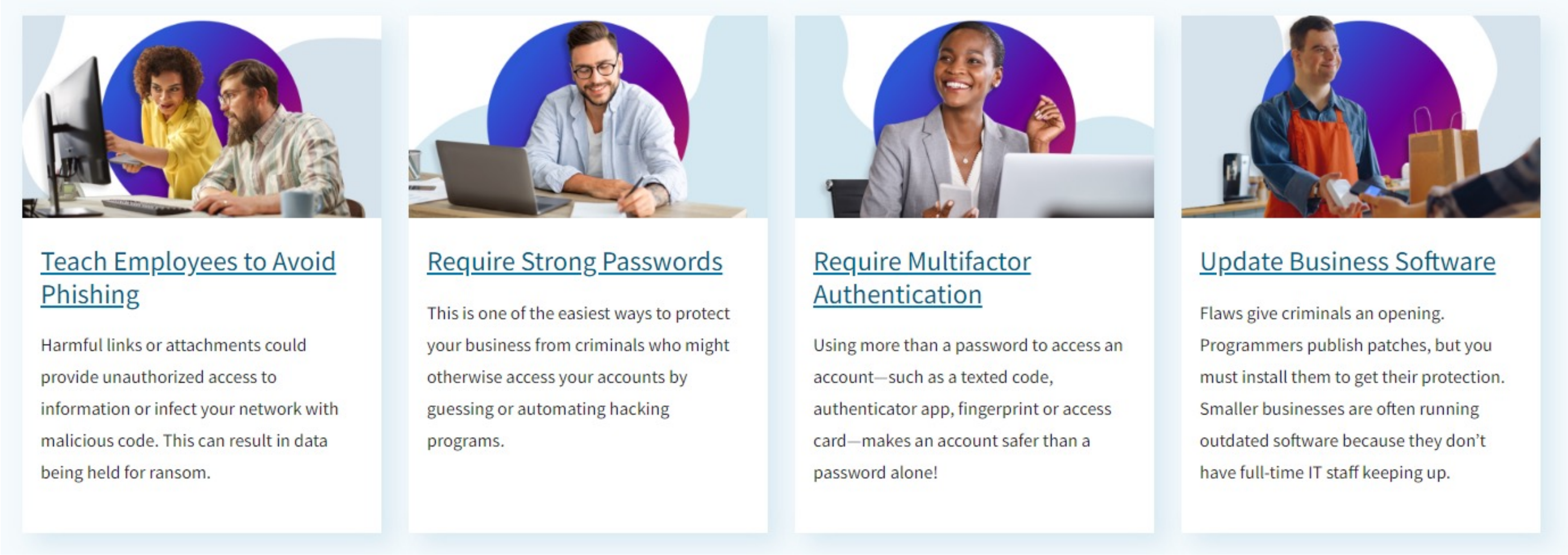
[3] Joint FBI-CISA-EPA-NSA Cybersecurity Advisory: Ongoing Cyber Threats to U.S. Water and Wastewater Systems

This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.

TLP:CLEAR

Lauren Wisniewski
March 7, 2024

Secure Our World – Secure Your Business



Teach Employees to Avoid Phishing

Harmful links or attachments could provide unauthorized access to information or infect your network with malicious code. This can result in data being held for ransom.

Require Strong Passwords

This is one of the easiest ways to protect your business from criminals who might otherwise access your accounts by guessing or automating hacking programs.

Require Multifactor Authentication

Using more than a password to access an account—such as a texted code, authenticator app, fingerprint or access card—makes an account safer than a password alone!

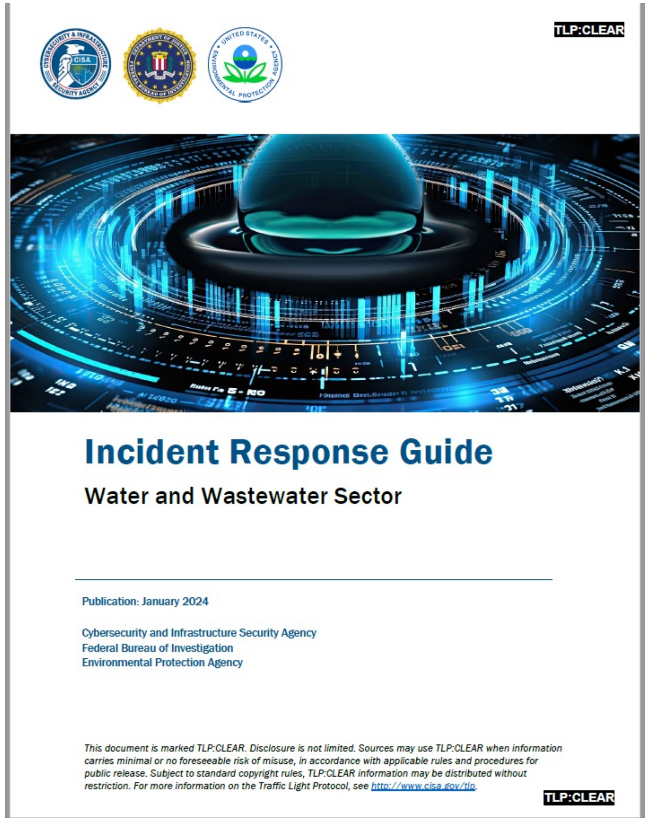
Update Business Software

Flaws give criminals an opening. Programmers publish patches, but you must install them to get their protection. Smaller businesses are often running outdated software because they don’t have full-time IT staff keeping up.

https://www.cisa.gov/secure-our-world/secure-your-business

Water and Wastewater Sector Incident Response Guide

- This Guide 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.
- The Guide:
  1. Establishes clear guidance for reporting cyber incidents
  2. Connects utilities with available cybersecurity resources, services, and no-cost trainings
  3. Empowers utilities to build a strong cybersecurity baseline to improve cyber resilience and cyber hygiene
  4. Encourages utilities to integrate into their local cyber communities



TLP:CLEAR

Incident Response Guide

Water and Wastewater Sector

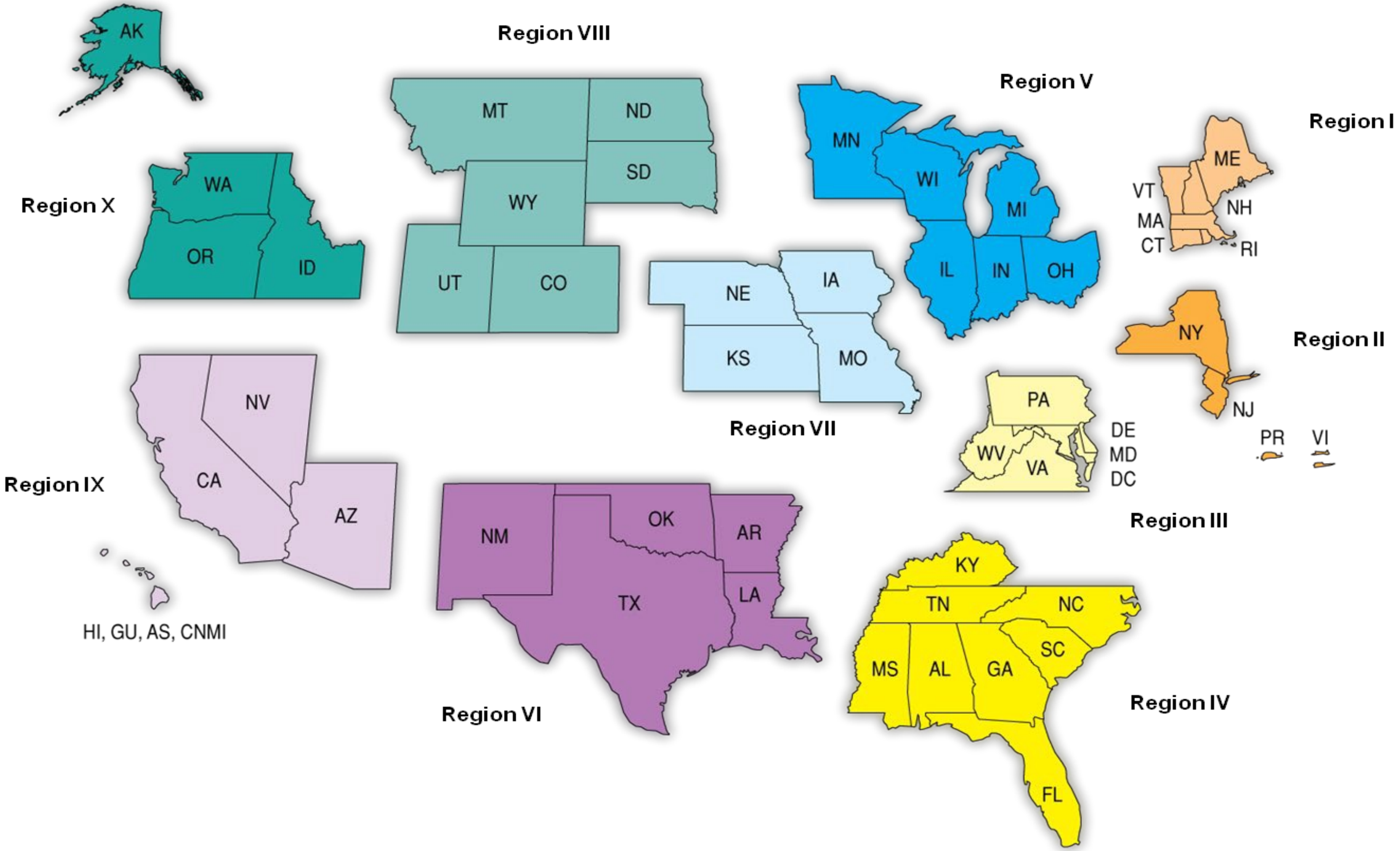
Publication: January 2024

Cybersecurity and Infrastructure Security Agency
Federal Bureau of Investigation
Environmental Protection Agency

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.cisa.gov/tlp.

TLP:CLEAR

Regionally Deployed Personnel



Regional Personnel:

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

Cybersecurity Services (Voluntary & No Cost)

Strategic

- Cyber Resilience Review (CRR)
- External Dependencies Management (EDM)
- Cyber Infrastructure Survey (CIS)
- Ransomware Readiness Assessment (RRA)
- Cyber Tabletop Exercises (CTTX)
- Cross-Sector Cybersecurity Performance Goals (CPGs)

Tactical

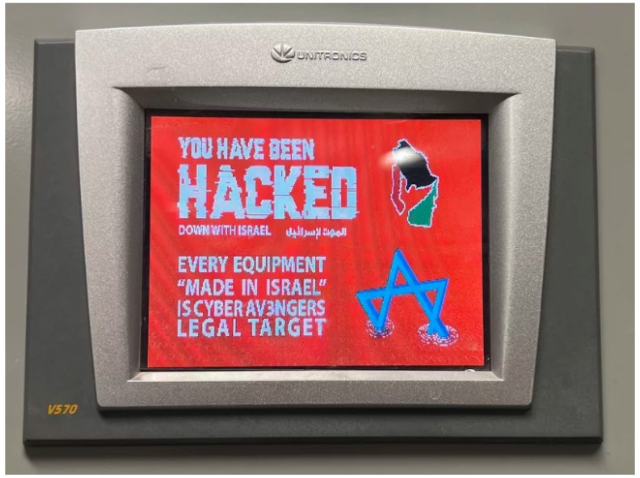
- Vulnerability Scanning
- Known Exploited Vulnerabilities (KEV)
- Cyber Security Evaluation Tool (CSET)

STRATEGIC
(C-Suite Level)

TECHNICAL
(Network/System Admin Level)

Report Cyber Incidents

- cisa.gov/report
- Email: report@cisa.gov
- Call 888-282-0870



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

Questions & Contact Info

Contact Information

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