

CISA CYBERSECURITY AWARENESS

Travis Light
Cybersecurity Advisor, Montana



CISA

**CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY**

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American people.

MISSION

Lead the national effort to understand, manage, and reduce risk to the nation's cyber and physical infrastructure.



CISA

STRATEGIC PLAN 2023–2025



GOAL 1

CYBER DEFENSE:

Spearhead the National Effort to Ensure Defense and Resilience of Cyberspace

GOAL 2

RISK REDUCTION & RESILIENCE:

Reduce Risks to, and Strengthen Resilience of, America's Critical Infrastructure

GOAL 3

OPERATIONAL COLLABORATION:

Strengthen Whole-of-Nation Operational Collaboration and Information Sharing

GOAL 4

AGENCY UNIFICATION:

Unify as One CISA Through Integrated Functions, Capabilities, and Workforce

CISA's Core Capabilities

AT A GLANCE



PARTNERSHIP DEVELOPMENT



INFORMATION AND DATA SHARING



CAPACITY BUILDING



INCIDENT MANAGEMENT & RESPONSE



RISK ASSESSMENT AND ANALYSIS



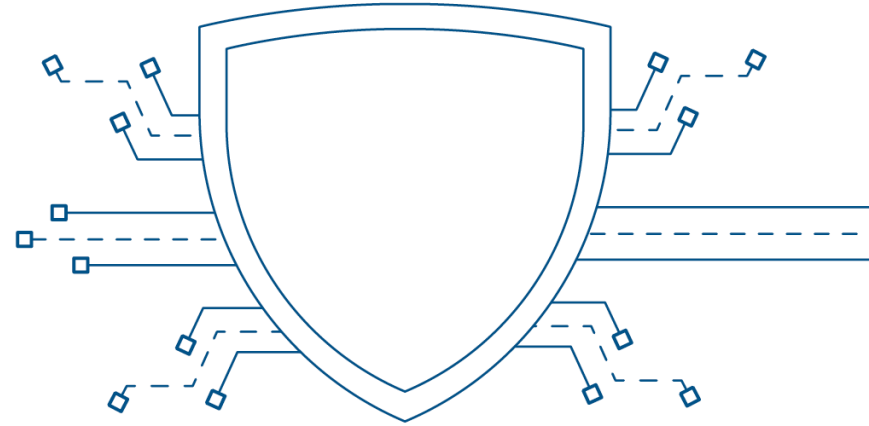
NETWORK DEFENSE



EMERGENCY COMMUNICATIONS



CISA's Cybersecurity Mission



HOW CISA IS CARRYING OUT ITS CYBERSECURITY MISSION:

- ▶ Mature Operational Collaboration
- ▶ Expand Operational Visibility
- ▶ Drive Progress to Secure Federal Civilian Networks
- ▶ Pursue Stronger Security at Scale
- ▶ Expand Access to CISA Capabilities

CYBERSECURITY MISSION

CISA drives and enables effective national cyber defense, resilience of national critical functions, and a robust supporting ecosystem.



CISA's Infrastructure Security Mission



HOW CISA IS CARRYING OUT ITS INFRASTRUCTURE SECURITY MISSION:

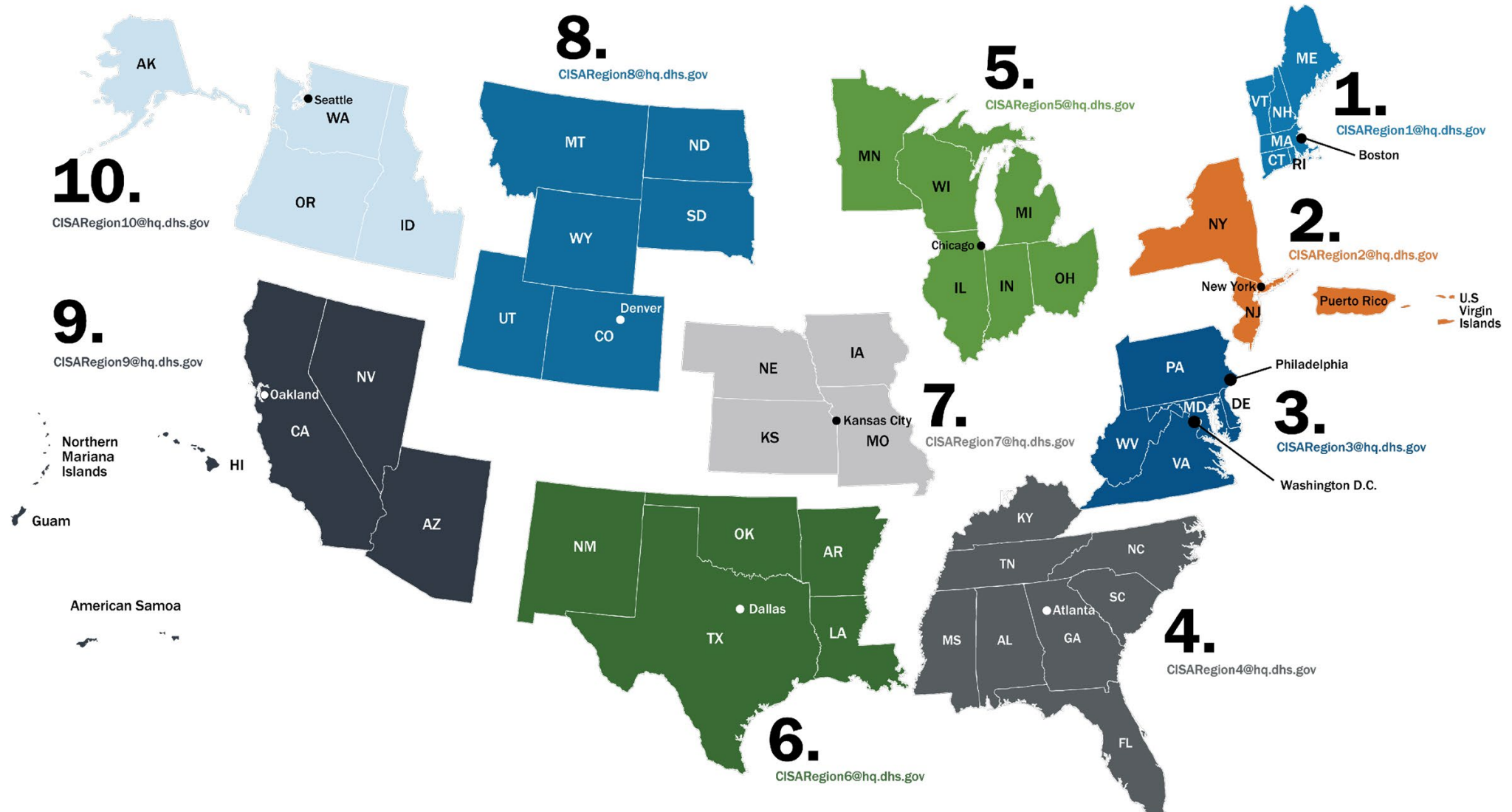
- ▶ Combat Domestic Violent Extremism
- ▶ Refreshing the National Infrastructure Protection Plan (The National Plan) and Implementing the 2021 National Defense Authorization Act (NDAA) Section 9002
- ▶ Chemical Security

INFRASTRUCTURE SECURITY MISSION

CISA leads the coordinated effort to reduce risks posed to our critical infrastructure, whether from man-made or natural causes.

CISA Regions

- 1 Boston, MA
- 2 New York, NY
- 3 Philadelphia, PA
- 4 Atlanta, GA
- 5 Chicago, IL
- 6 Dallas, TX
- 7 Kansas City, MO
- 8 Denver, CO
- 9 Oakland, CA
- 10 Seattle, WA



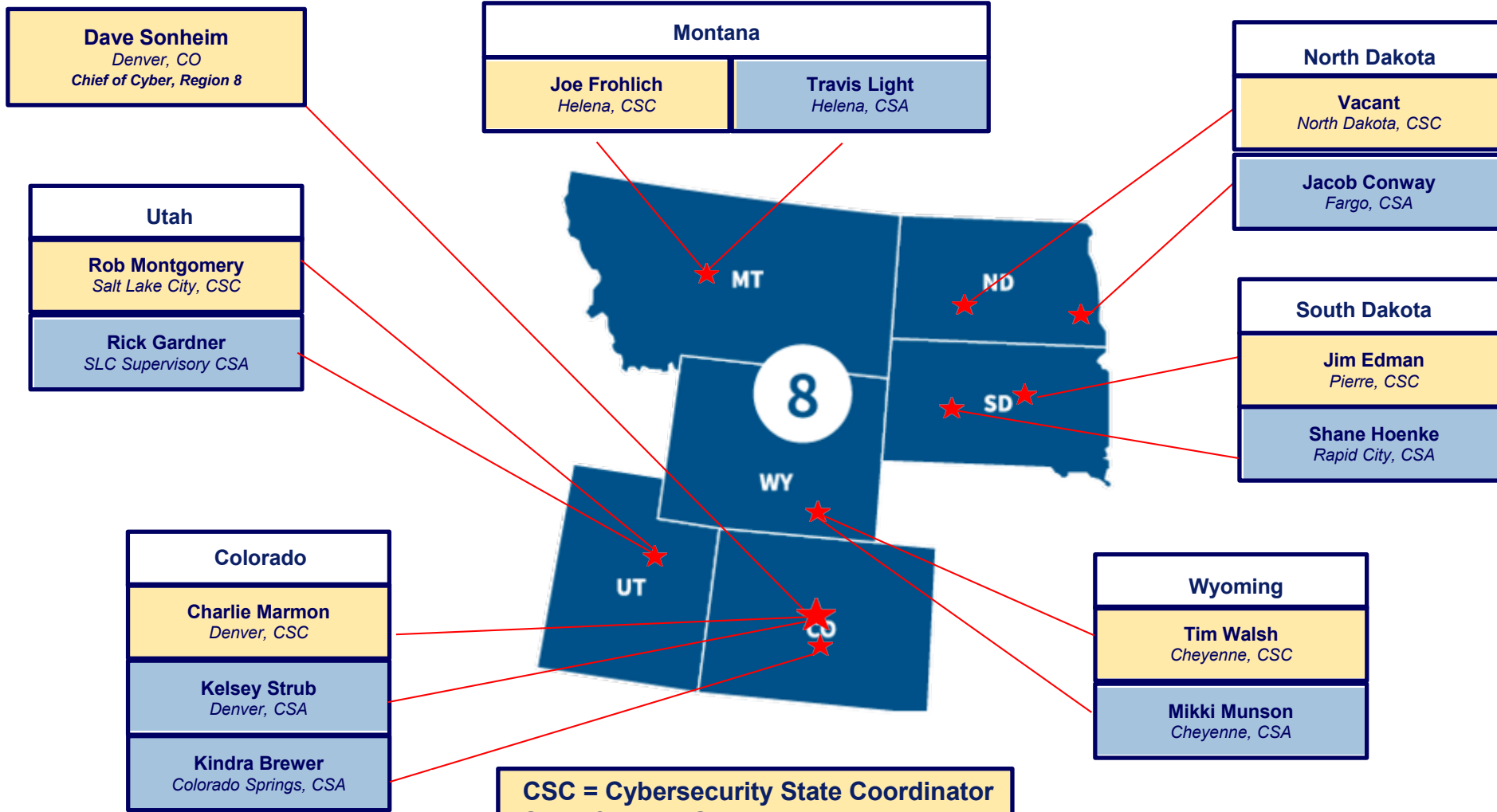
Cybersecurity Advisor Program

Cybersecurity Advisors (CSAs) support CISA's Cybersecurity Mission in the following areas:

- **Assess:** Evaluate critical infrastructure cyber risk.
- **Promote:** Encourage best practices and risk mitigation strategies.
- **Build:** Initiate, develop capacity, and support cyber communities-of-interest and working groups.
- **Educate:** Inform and raise awareness.
- **Listen:** Collect stakeholder requirements.
- **Coordinate:** Bring together incident support and lessons learned.



CISA Region 8 – Cyber Cadre




















**CSC = Cybersecurity State Coordinator
State & Local Government**

**CSA = Cybersecurity Advisor
Critical Infrastructure Focus**



16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

 CHEMICAL	CISA	 FINANCIAL	Treasury
 COMMERCIAL FACILITIES	CISA	 FOOD & AGRICULTURE	USDA & HHS
 COMMUNICATIONS	CISA	 GOVERNMENT FACILITIES	DHS & GSA
 CRITICAL MANUFACTURING	CISA	 HEALTHCARE & PUBLIC HEALTH	HHS
 DAMS	CISA	 INFORMATION TECHNOLOGY	CISA
 DEFENSE INDUSTRIAL BASE	DOD	 NUCLEAR REACTORS, MATERIALS AND WASTE	CISA
 EMERGENCY SERVICES	CISA	 TRANSPORTATIONS SYSTEMS	TSA & USCG
 ENERGY	DOE	 WATER	EPA



[Water and Wastewater Systems](#)

Access to clean, healthy water is a requirement for all human activity. Protecting the systems that provide water is of vital importance to the stability and health of the nation and is the mission of the Water and Wastewater Systems Sector.



CISA/EPA – Boosting Water Sector Cybersecurity

*“We’ve seen a change in the adversarial landscape. We’re not just talking about nation-states – China, Russia, Iran, North Korea – but we’re seeing cyber criminals, cyber terrorist organizations also causing harm here in the United States. We’re seeing a change in the victim landscape. We’re not just talking about large cities and large municipalities, **but small rural water utilities are equally potential victims from these actors.** That combination – changes in the adversary and victim – really set up an environment where the threat landscape is changing. We need to be prepared across the nation.”*

- CISA Deputy Director Nitin Natarajan









CISA/EPA – Boosting Water Sector Cybersecurity

*“It’s important to dispel a myth about cybersecurity up front, that implementing a cybersecurity program against these evolving threats means you need to have IT or OT expertise or need to spend a small fortune on equipment or a consulting firm. In reality, **for most cyber attacks we’ve seen in the water sector, whether from cyber criminals or sophisticated state actors, the adoption of basic cybersecurity practices would have thwarted the attack.**”*

- David Travers, EPA Director, Water Infrastructure & Cyber Resilience Division



Threat Actors and Motivation

	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
THREATS						
MOTIVATION	Hackers use computer network exploitation to advance their political or social causes.	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.	Trusted insiders steal proprietary information for personal, financial, and ideological reasons.	Nation-state actors conduct computer intrusions to steal sensitive state secrets and propriety information from private companies.	Terrorist groups sabotage the computer systems that operate our critical infrastructure, such as the electric grid.	Nation-state actors sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.



The Threat is Real



OFFICE of INTELLIGENCE and ANALYSIS

INTELLIGENCE IN FOCUS

24 OCTOBER 2023

DHS-IA-IF-2023-18159

CYBERSECURITY

(U//FOUO) Malicious Cyber Actors Likely View US Water and Wastewater Systems Sector as an Attractive Target

(U//FOUO) Malicious cyber actors likely view US Water and Wastewater Systems (WWS) infrastructure as an attractive target due to the sector's segmented nature and cybersecurity-related resource challenges. Since 2020, malicious cyber actors reportedly gained access to the business and operational technology networks of the US WWS sector using relatively unsophisticated techniques, with attacks resulting in the encryption, exfiltration, or deletion of sensitive data. WWS utilities require significant physical, digital, and human resources to safely operate, and the sector faces challenges related to maintaining and protecting its systems.



Travis Light
March 20, 2024

The Threat is Real

Thanksgiving 2023

- Iran-affiliated “CyberAv3ngers” group targeted Israeli-manufactured Unitronics PLCs
- Dozens of utilities were hacked
- Affected utilities encountered this message →
- Every compromised device used “out-of-the-box” configurations. Default passwords, default port, and directly accessible via the internet
- Takeaway: **Change default configuration**



Iran-linked cyberattacks threaten equipment used in U.S. water systems and factories

UPDATED DECEMBER 2, 2023 · 1:51 PM ET

 Juliana Kim



This photo provided by the Municipal Water Authority of Aliquippa shows the screen of a Unitronics device that was hacked in Aliquippa, Pa., on Nov. 25.

Travis Light
March 20, 2024

The Threat is Real



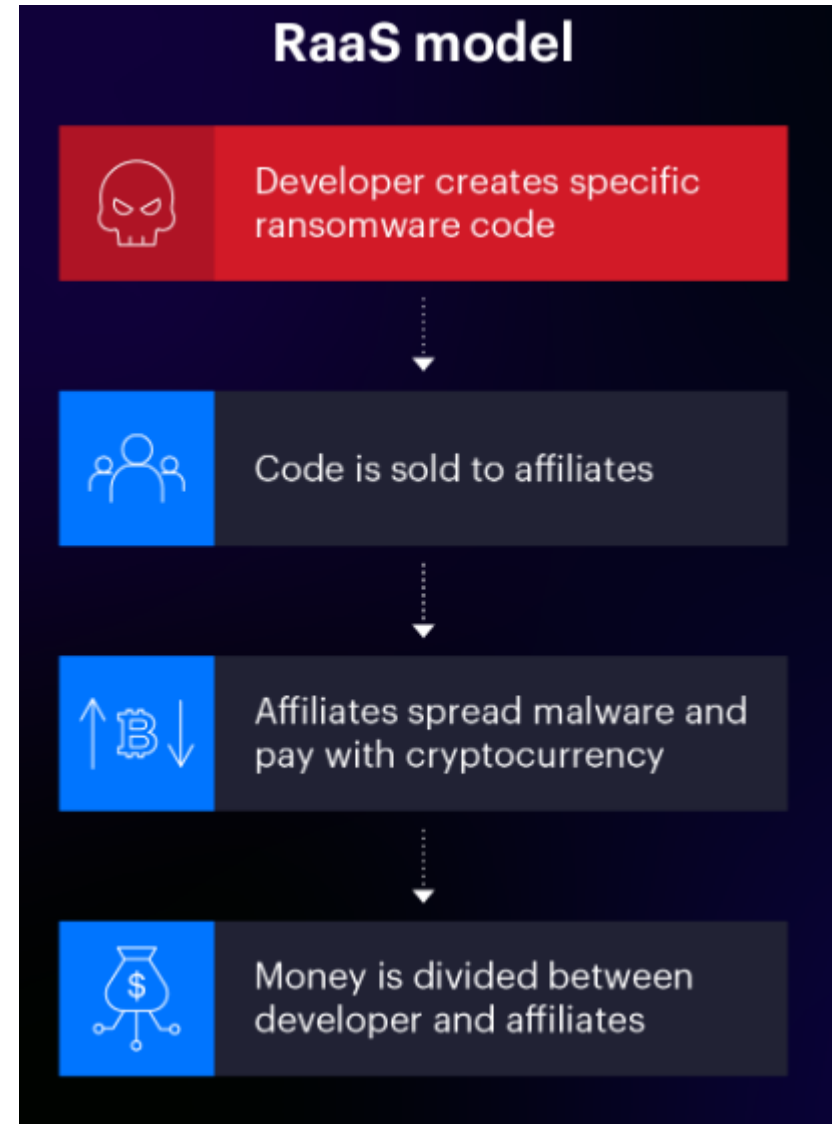
January 2024

- Pro-Russian hactivists compromised two US water utilities
- Remotely caused water distribution systems to overflow
- Posted video on their social media channels of the manipulation
- Takeaway: “likely were opportunistic and not the result of advanced skills or tactics, **underscoring the importance of basic cyber hygiene**”



Ransomware-as-a-Service (RaaS) Model

- Ransomware as a Service (RaaS) is a business model between ransomware operators and affiliates in which **affiliates pay to launch ransomware attacks developed by operators.**
- Popularity increases → Barriers to entry drop, becomes scalable, more efficient.
- Enables relatively unskilled bad actors to access complex tools and the environment from which to run their campaigns.
- Increased investment in many of the platforms themselves, upgrading their core ransomware systems to stay ahead of the good guys and evade detection.



CISA/EPA W/WS Cybersecurity Toolkit

- Published January 30th
- Consolidates CISA and EPA resources such as:
 - [CISA Vulnerability Scanning](#)
 - EPA [Cybersecurity Incident Response Helpdesk](#)
 - Cybersecurity Assessment Services
 - Cybersecurity Planning Guides
 - Templates and Best Practices
 - Information Sharing
 - Funding Opportunities



[Link to CISA/EPA Toolkit](#)

Travis Light
March 20, 2024

CISA/EPA/FBI Top Cyber Actions for W/WS



Published February 23rd

[Top Cyber Actions for Securing Water Systems](#)

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.



[Link to CISA/EPA Toolkit](#)

Travis Light
March 20, 2024

CISA/EPA/FBI Top Cyber Actions for W/WS



Published February 23rd

[Top Cyber Actions for Securing Water Systems](#)

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 mitigating vulnerabilities in both OT and IT networks.



[Link to CISA/EPA Toolkit](#)

Travis Light
March 20, 2024

CISA/EPA/FBI Top Cyber Actions for W/WS



Published February 23rd

[Top Cyber Actions for Securing Water Systems](#)

3. Change Default Passwords Immediately

Require unique, strong, and complex passwords for all water systems, including connected infrastructure. Weak default or insecure passwords are easy to discover and exploit, and they may allow cyber threat actors to make changes to a water systems' operational processes. This can negatively impact public health and safety. Change default or insecure passwords and implement multifactor authentication (MFA) where possible.



[Link to CISA/EPA Toolkit](#)

Travis Light
March 20, 2024

CISA/EPA/FBI Top Cyber Actions for W/WS



Published February 23rd

[Top Cyber Actions for Securing Water Systems](#)

4. Conduct an Inventory of OT/IT Assets

Create an inventory of software and hardware assets to help understand what you need to protect. Focus initial efforts on internet-connected devices and devices where manual operations are not possible. Use monitoring to identify the devices communicating on your network.



[Link to CISA/EPA Toolkit](#)

Travis Light
March 20, 2024

CISA/EPA/FBI Top Cyber Actions for W/WS



Published February 23rd
[Top Cyber Actions for Securing Water Systems](#)

5. Develop and Exercise Cybersecurity Incident Response and Recovery Plans

Develop

Understand incident response actions, roles, responsibilities, as well as who to contact and how to report a cyber incident before one occurs to ensure readiness against potential targeting.

Exercise

Test your incident response plan annually to ensure all operators are familiar with roles and responsibilities.



[Link to CISA/EPA Toolkit](#)

Travis Light
March 20, 2024

CISA/EPA/FBI Top Cyber Actions for W/WS



Published February 23rd

[Top Cyber Actions for Securing Water Systems](#)

6. Backup OT/IT Systems

Regularly backup OT/IT systems so you can recover to a known and safe state in the event of a compromise. Test backup procedures and isolate backups from network connections. Implement the NIST 3-2-1 rule:

- 3) Keep three copies: one primary and two backups;
- 2) Keep the backups on two different media types;
- 1) Store one copy offsite.



[Link to CISA/EPA Toolkit](#)

CISA/EPA/FBI Top Cyber Actions for W/WS



Published February 23rd

[Top Cyber Actions for Securing Water Systems](#)

7. Reduce Exposure to Vulnerabilities

Mitigate known vulnerabilities and keep all systems up to date with patches and security updates. Prioritize OT patches in accordance with [CISA's Known Exploited Vulnerabilities \(KEV\) catalog](#) during scheduled downtime of OT equipment; prioritize patches in IT, as applicable. [CISA's Secure our World Campaign](#) provides guidance on updating software.



[Link to CISA/EPA Toolkit](#)

Travis Light
March 20, 2024

CISA/EPA/FBI Top Cyber Actions for W/WS



Published February 23rd

[Top Cyber Actions for Securing Water Systems](#)

8. Conduct Cybersecurity Awareness Training

Conduct cybersecurity awareness training annually, at a minimum, to help all employees understand the importance of cybersecurity and how to prevent and respond to cyberattacks.



[Link to CISA/EPA Toolkit](#)

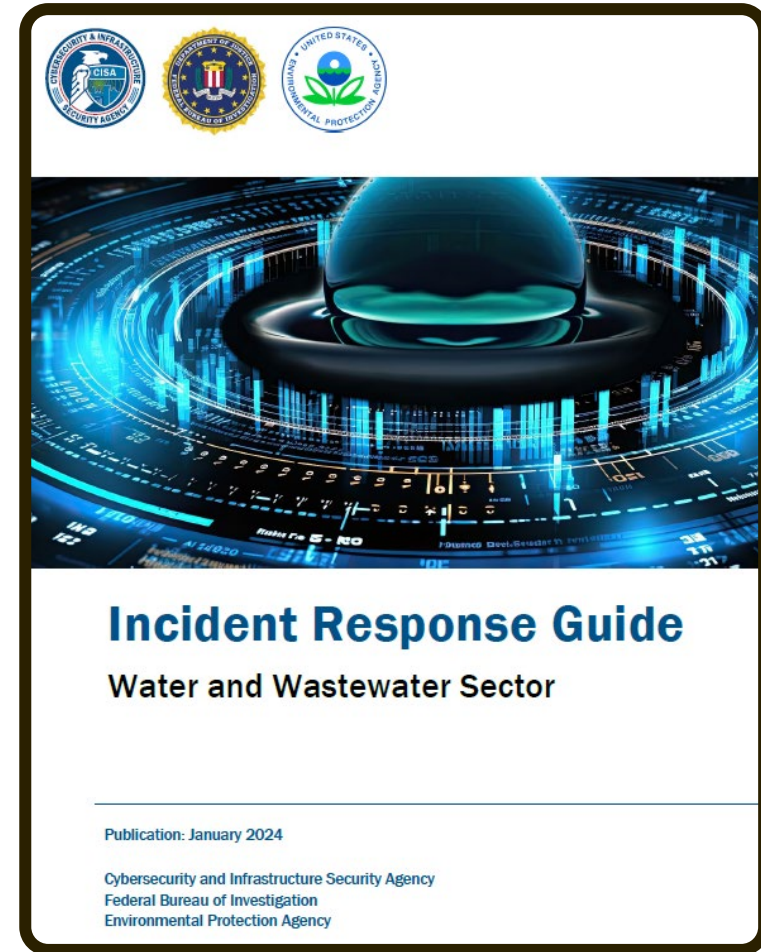
Travis Light
March 20, 2024

CISA/EPA/FBI Incident Response Guide

Guides your utility in building your Incident Response Plan

Resources and tips for each step in the IR Process:

- Preparation
- Detection & Analysis
- Containment, Eradication, & Recovery
- Post-Incident Activity



[Link to Incident Response Guide](#)

Travis Light
March 20, 2024

Protected Critical Infrastructure Information Program

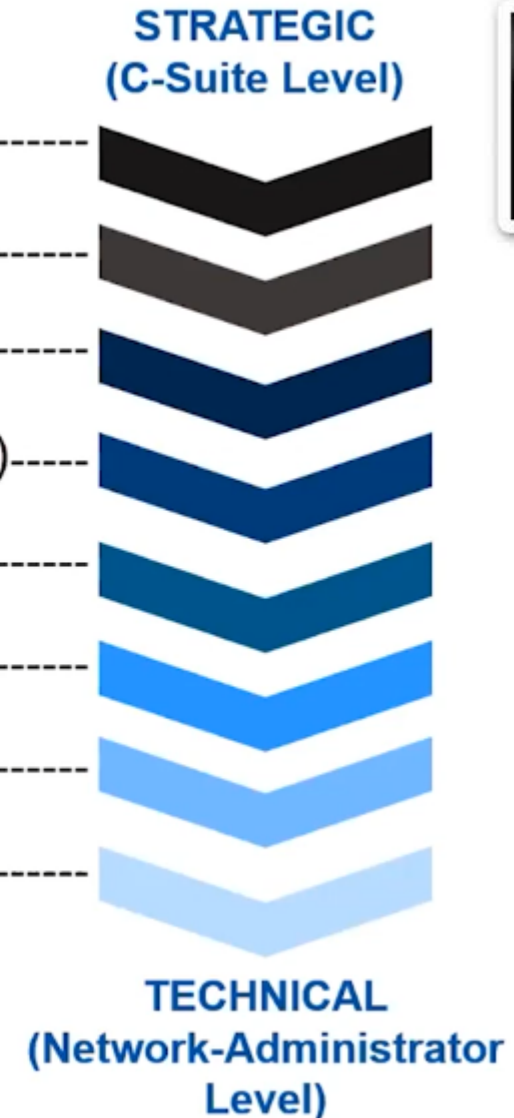
Protected Critical Infrastructure Information (PCII) Program Guards Your Information

- Sensitive critical infrastructure information voluntarily given to CISA is protected by law from
 - Public release under Freedom of Information Act requests,
 - Public release under State, local, tribal, or territorial disclosure laws,
 - Use in civil litigation and
 - Use in regulatory purposes.
- To learn more, visit www.dhs.gov/pcii



Cybersecurity Resources and Assessments

- Cyber Resilience Review (Strategic) -----
- External Dependencies Management (Strategic) -----
- Cyber Infrastructure Survey (Strategic) -----
- Cybersecurity Evaluations Tool (Strategic/Technical) -----
- Phishing Campaign Assessment (Technical) -----
- ★ Vulnerability Scanning / Hygiene (Technical) -----
- Validated Architecture Design Review (Technical) -----
- Risk and Vulnerability Assessment (Technical) -----

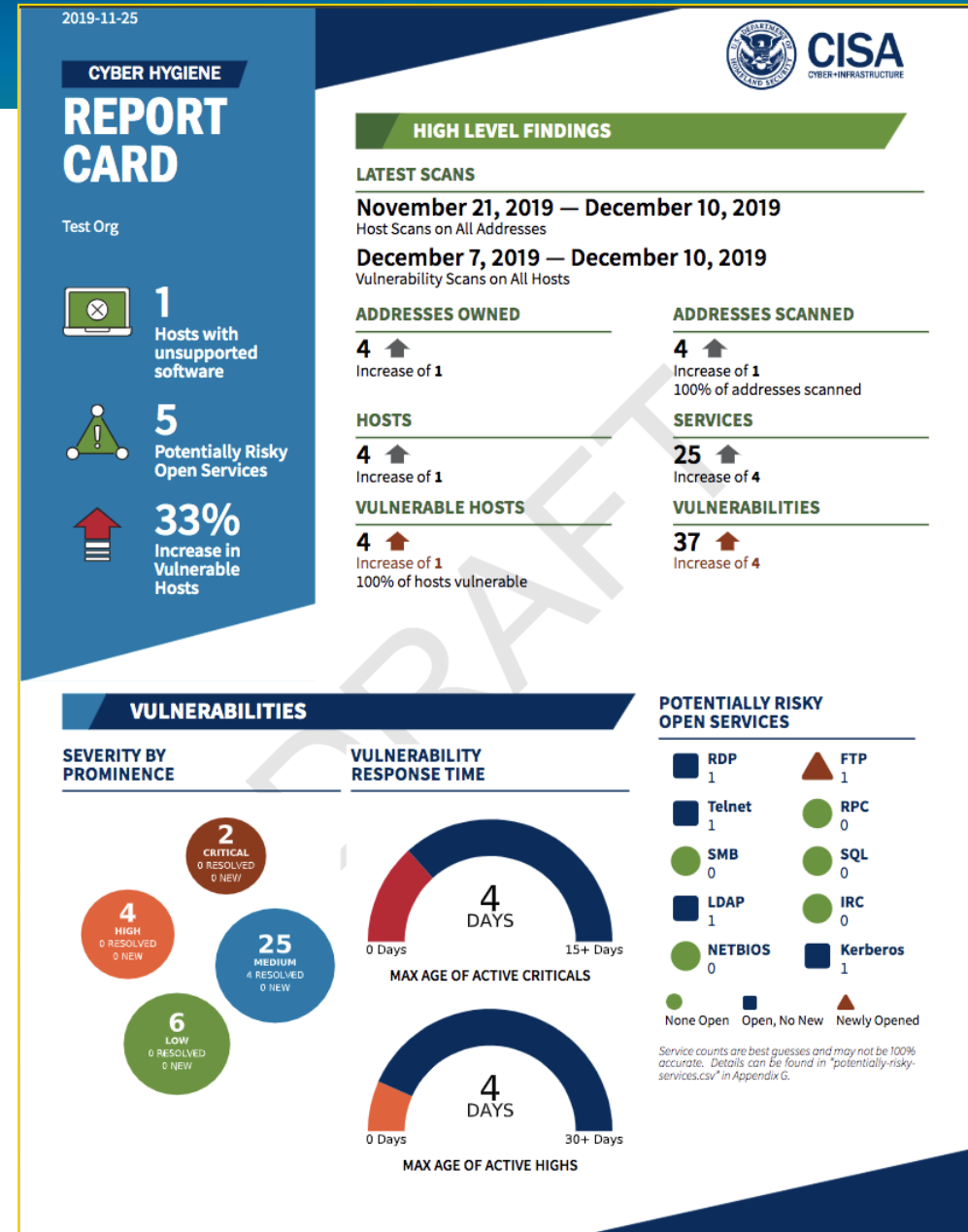


Vulnerability Scanning

- Automated scanning of **External-facing, Internet accessible** systems (Top 1000 Ports, can include cloud sites)
- **Weekly report** card that includes current scan results, historic trends, Known Exploited Vulnerabilities, and comparisons to the national average
- Helps you understand your unique exposure
- **Know what the Internet already knows about your environment!**



Sign up by emailing
vulnerability@cisa.dhs.gov
with subject line
“Requesting Cyber Hygiene Services”



#StopRansomware



Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. [StopRansomware.gov](https://www.stopransomware.gov) is the U.S. Government's official one-stop location for resources to tackle ransomware more effectively.



Travis Light
March 20, 2024

Cyber Tabletop Exercises (CTTX)

- May 14th, Billings – MSU Spring Water School
 - CISA will lead a Cyber Incident Response Tabletop Exercise as part of the event
 - Additional opportunity during Fall Water School
- Use CISA Tabletop Exercise Packages (CTEP) to help develop your own
 - [Water & Wastewater Systems Cyber CTEP Situation Manual](#)
 - [Industrial Controls CTEP Situation Manual](#)
 - [Ransomware CTEP Situation Manual](#)
 - [Ransomware Third Party Vendor CTEP Situation Manual](#)
 - [Vendor Phishing CTEP Situation Manual](#)
 - [Local Governments CTEP Situation Manual](#)



[CISA Tabletop Exercise Packages \(CTEPs\)](#)

Information Sharing Opportunities



[Join WaterISAC](#)

[About WaterISAC](#)



American Water Works Association

Dedicated to the World's Most Vital Resource

[AWWA Cyber Resilience Resources](#)



ONG-ISAC



National Defense ISAC



RETAIL & HOSPITALITY ISAC



Travis Light
March 20, 2024

Protective Security Advisor (PSA)



- **INFRASTRUCTURE SURVEY TOOL** - Identifying facilities' physical security, security forces, security management, information sharing, protective measures, and dependencies related to preparedness, mitigation, response, resilience, and recovery;
- **Assist Visit** – Identifies and recommends protective measures at facilities, provide comparison across like assets, and track implementation of new protective measures.
- **Infrastructure Visualization Platform (IVP)** – brings a facility's digital floorplans to life by placing on it 360° panoramic photographs, immersive video, geospatial information, and hypermedia data of critical facilities, surrounding areas, and transportation routes that assist with security planning, protection, and response efforts.
- **SAFE Tool** The Security Assessment at First Entry (SAFE) tool is designed to assess the current security posture and identify options for facility owners and operators to mitigate relevant threats



CISA Protective Security Advisors

Travis Light
March 20, 2024

Incident Reporting

Montana Analysis and Technical Information
Center (MATIC):
406-444-1318

CISA Central 24x7 contact number:
888-282-0870

[Report an Incident: www.cisa.gov/forms/report](https://www.cisa.gov/forms/report)



CISA – MT Contacts

TRAVIS LIGHT

Cybersecurity Advisor
Helena, MT
(406) 894-8374
travis.light@cisa.dhs.gov

JOE FROHLICH

Cybersecurity State Coordinator
Helena, MT
(406) 461-2651
joseph.frohlich@cisa.dhs.gov

ALBERT MENDOZA

Protective Security Advisor
Billings, MT
(406) 371-3585
albert.mendoza@cisa.dhs.gov

RANDY MIDDLEBROOK

Protective Security Advisor
Helena, MT
(406) 839-1165
randy.middlebrook@cisa.dhs.gov





For more information, visit [CISA.gov](https://www.cisa.gov) or contact central@cisa.dhs.gov