CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

CYBERSECURITY SERVICES FOR WATER & WASTEWATER SECTOR

ASSOCIATION OF ENVIRONMENTAL AUTHORITIES

UTILITY MANAGEMENT CONFERENCE

Formulas for SUCCESS

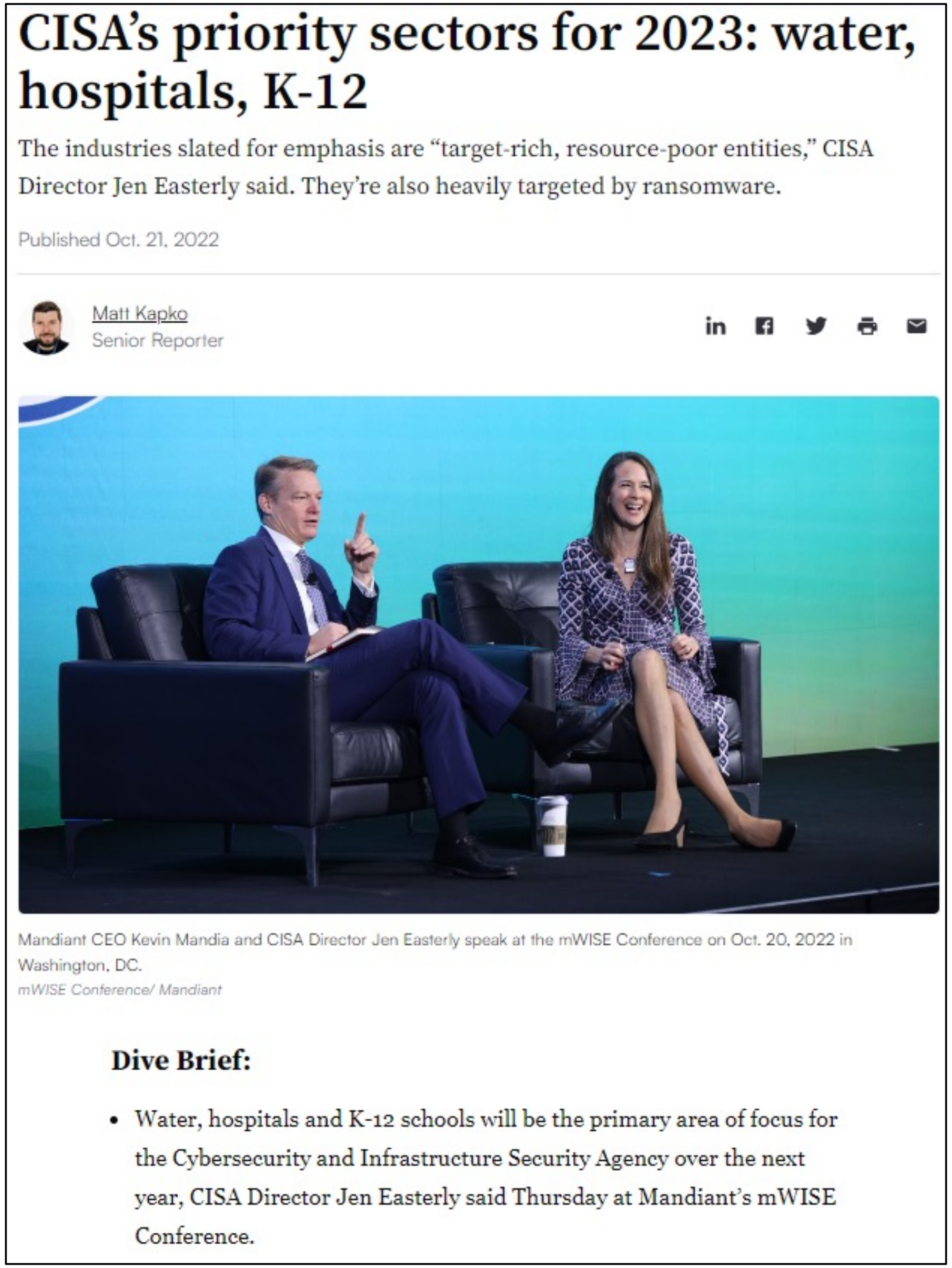
Christopher Kay
Cybersecurity State Coordinator, Region II
Cybersecurity and Infrastructure Security Agency

CISA

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

As America’s Cyber Defense Agency and the National Coordinator for critical infrastructure resiliency and security, CISA leads the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day.



CISA's priority sectors for 2023: water, hospitals, K-12

The industries slated for emphasis are "target-rich, resource-poor entities," CISA Director Jen Easterly said. They're also heavily targeted by ransomware.

Published Oct. 21, 2022

Matt Kapko
Senior Reporter

Mandiant CEO Kevin Mandia and CISA Director Jen Easterly speak at the mWISE Conference on Oct. 20, 2022 in Washington, DC.

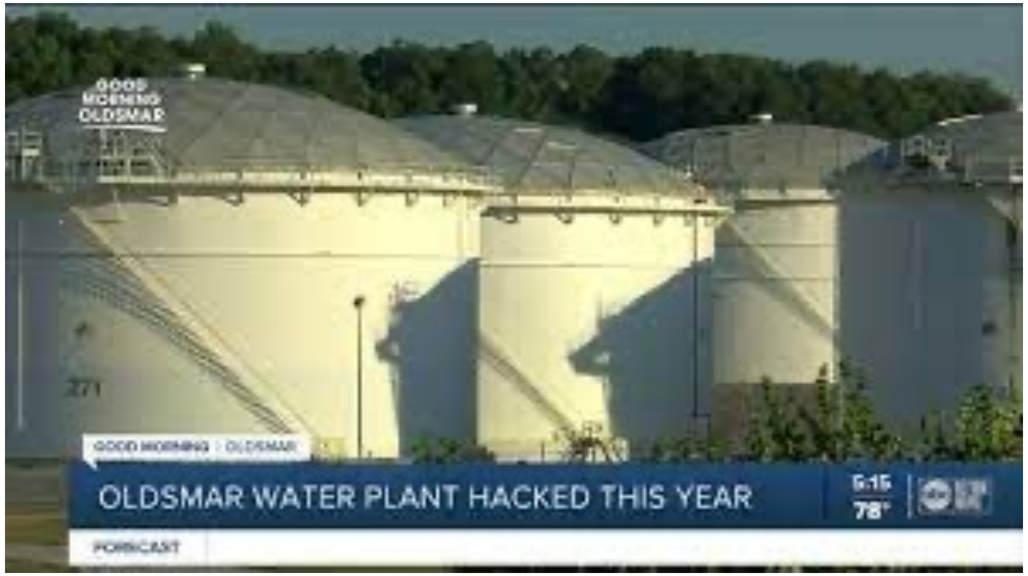
mWISE Conference/ Mandiant

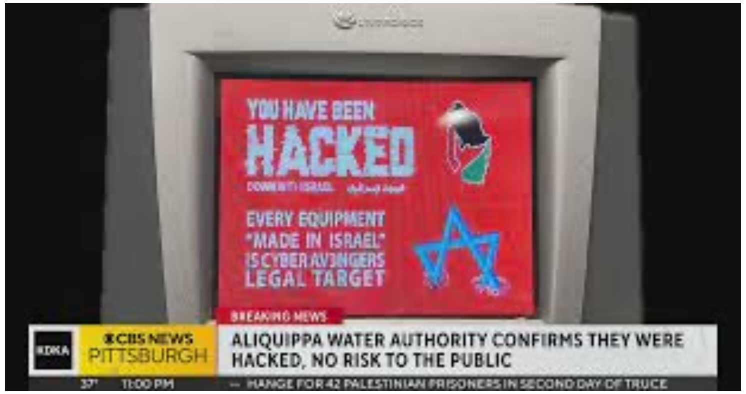
Dive Brief:

- Water, hospitals and K-12 schools will be the primary area of focus for the Cybersecurity and Infrastructure Security Agency over the next year, CISA Director Jen Easterly said Thursday at Mandiant's mWISE Conference.

What are the threats to critical infrastructure?

A Close Call: 2021 Hacking the Oldsmar Water System



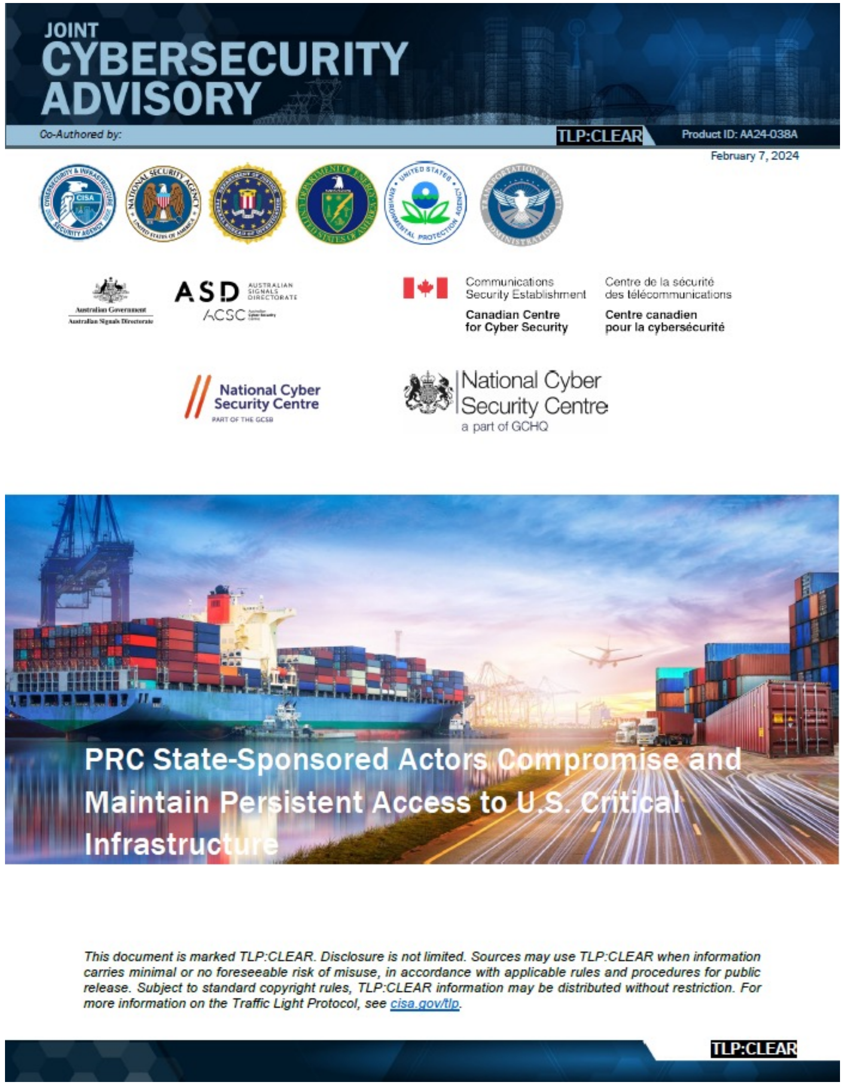


Christopher Kay
March 19, 2024

Who is behind these attacks?

Nation States and their proxies…

What are the threats to critical infrastructure?



JOINT CYBERSECURITY ADVISORY

Co-Authored by:

TLP:CLEAR

Product ID: AA24-038A

February 7, 2024

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
PART OF THE GCSB

National Cyber Security Centre
a part of GCHQ

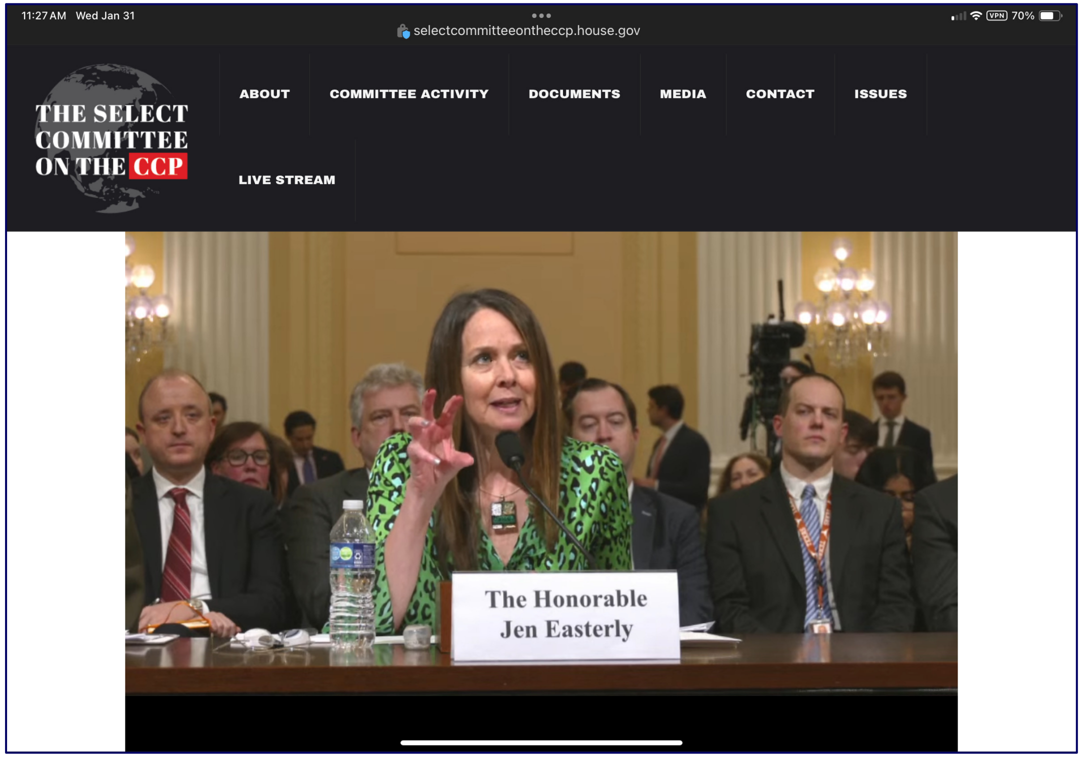
PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure

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 cisa.gov/tlp.

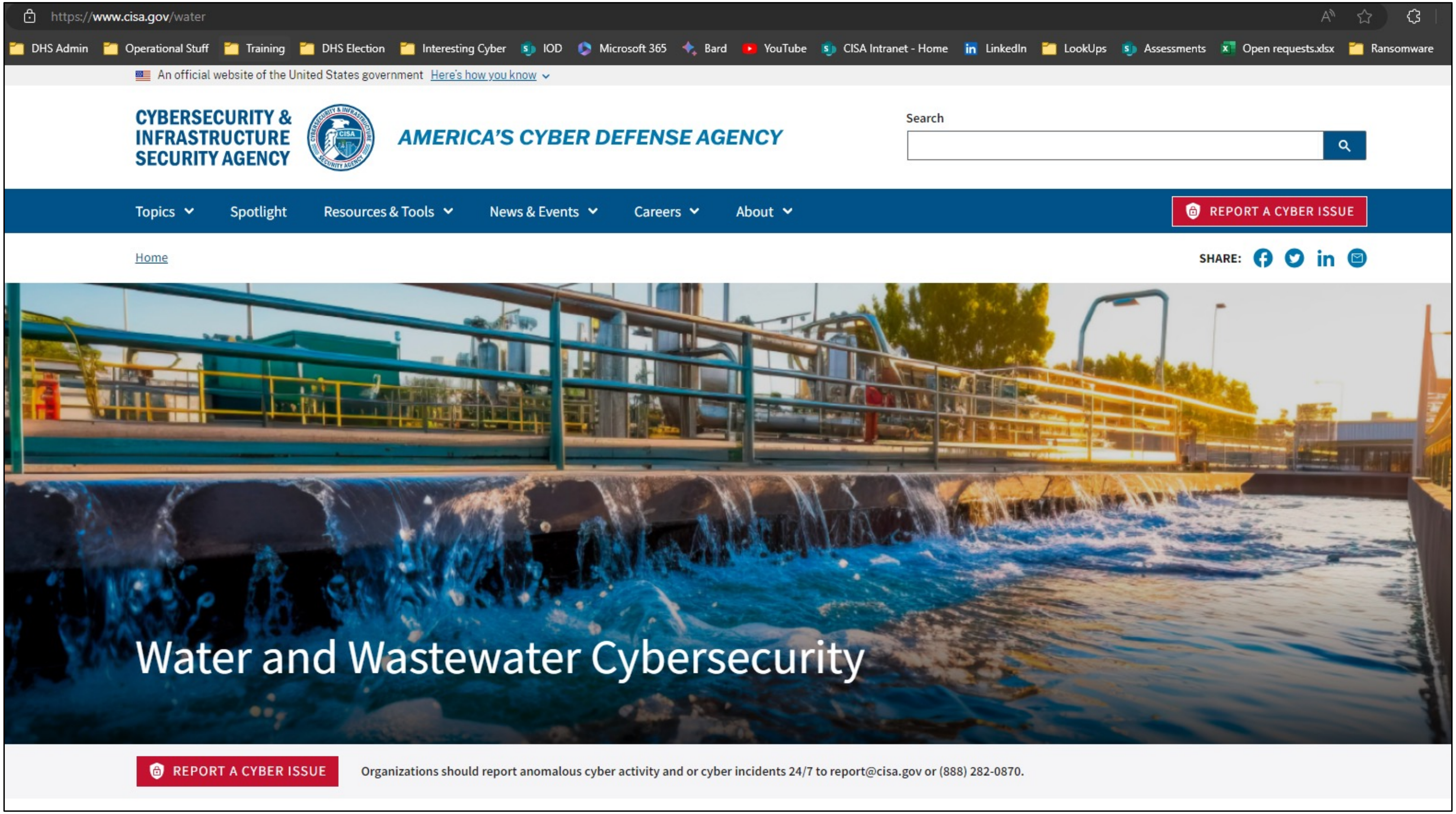
TLP:CLEAR

Christopher Kay
March 19, 2024

What are the threats to critical infrastructure?


11:27 AM Wed Jan 31
selectcommitteeontheccp.house.gov
70%
THE SELECT COMMITTEE ON THE CCP
ABOUT
COMMITTEE ACTIVITY
DOCUMENTS
MEDIA
CONTACT
ISSUES
LIVE STREAM
The Honorable Jen Easterly

> “Chinese hackers easily infiltrate infrastructure by exploiting known product defects, which are the result of companies prioritizing product features and speed to market over security.”
>
> -CISA Director Jen Easterly



An official website of the United States government Here's how you know

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

Water and Wastewater Cybersecurity

REPORT A CYBER ISSUE

Organizations should report anomalous cyber activity and or cyber incidents 24/7 to report@cisa.gov or (888) 282-0870.

www.cisa.gov/water

SELF-ASSESSMENTS

CSET Self-Assessments

- Cybersecurity Performance Goals Assessment
- Ransomware Readiness Assessment
- External Dependencies Management (Supply Chain Risk)
- Cyber Resilience Review (Comprehensive)
- American Water Works Association Cyber Infrastructure Survey
  - Compatible with the AWWA Cybersecurity Assessment Tool
- NIST SP 800-82 Rev 2 (Standard for ICS Systems)
- Incident Management Review

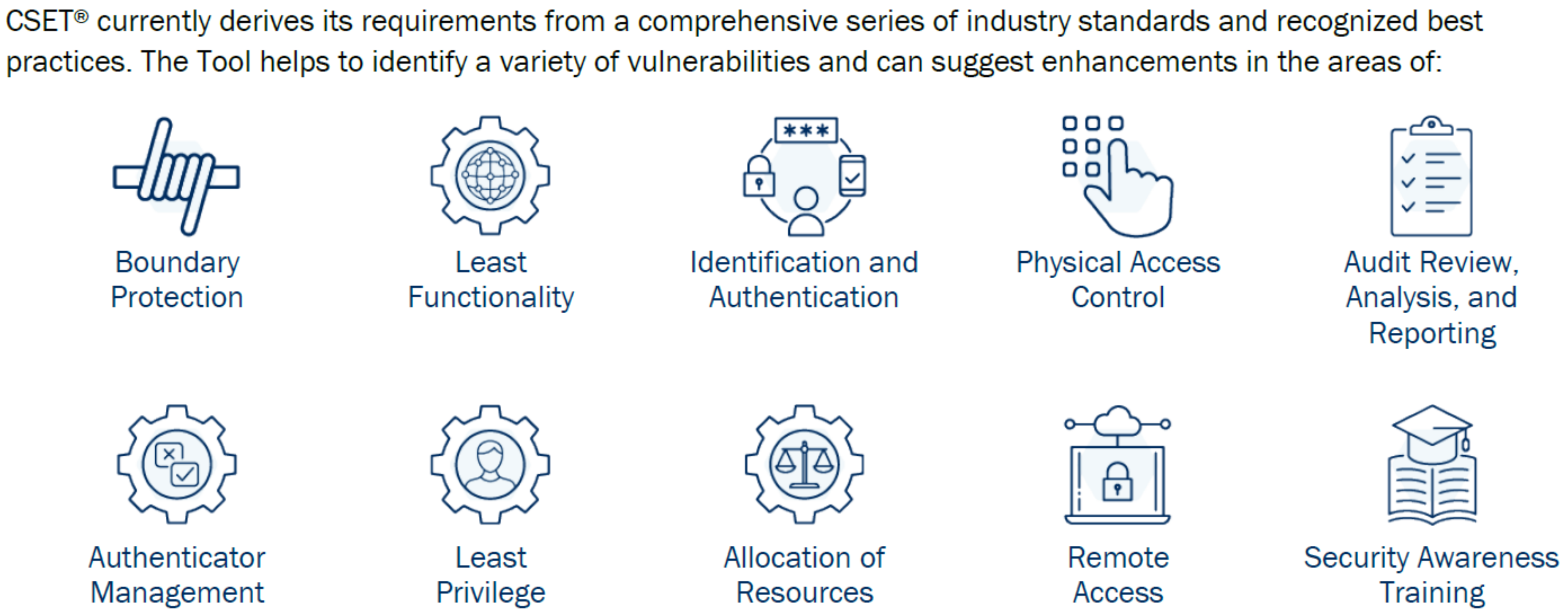
CSET®
CYBER SECURITY EVALUATION TOOL
U.S. DEPARTMENT OF HOMELAND SECURITY
CISA
CYBER+INFRASTRUCTURE

Cyber Security Evaluation Tool: CPGs

- **Cross-Sector Cybersecurity Performance Goals (CPG):** Assesses control system and information technology network security practices against industry standards.
- **Facilitated:** Self-Administered, undertaken independently
- **Benefits:**
  - Immediately available for download upon request
  - Understanding of operational technology and information technology network security practices
  - Ability to drill down on specific areas and issues
  - Helps to integrate cybersecurity into current corporate risk management strategy

Cyber Security Evaluation Tool: CPGs

- **Cross-Sector Cybersecurity Performance Goals (CPG)**



CSET® currently derives its requirements from a comprehensive series of industry standards and recognized best practices. The Tool helps to identify a variety of vulnerabilities and can suggest enhancements in the areas of:

Boundary Protection

Least Functionality

Identification and Authentication

Physical Access Control

Audit Review, Analysis, and Reporting

Authenticator Management

Least Privilege

Allocation of Resources

Remote Access

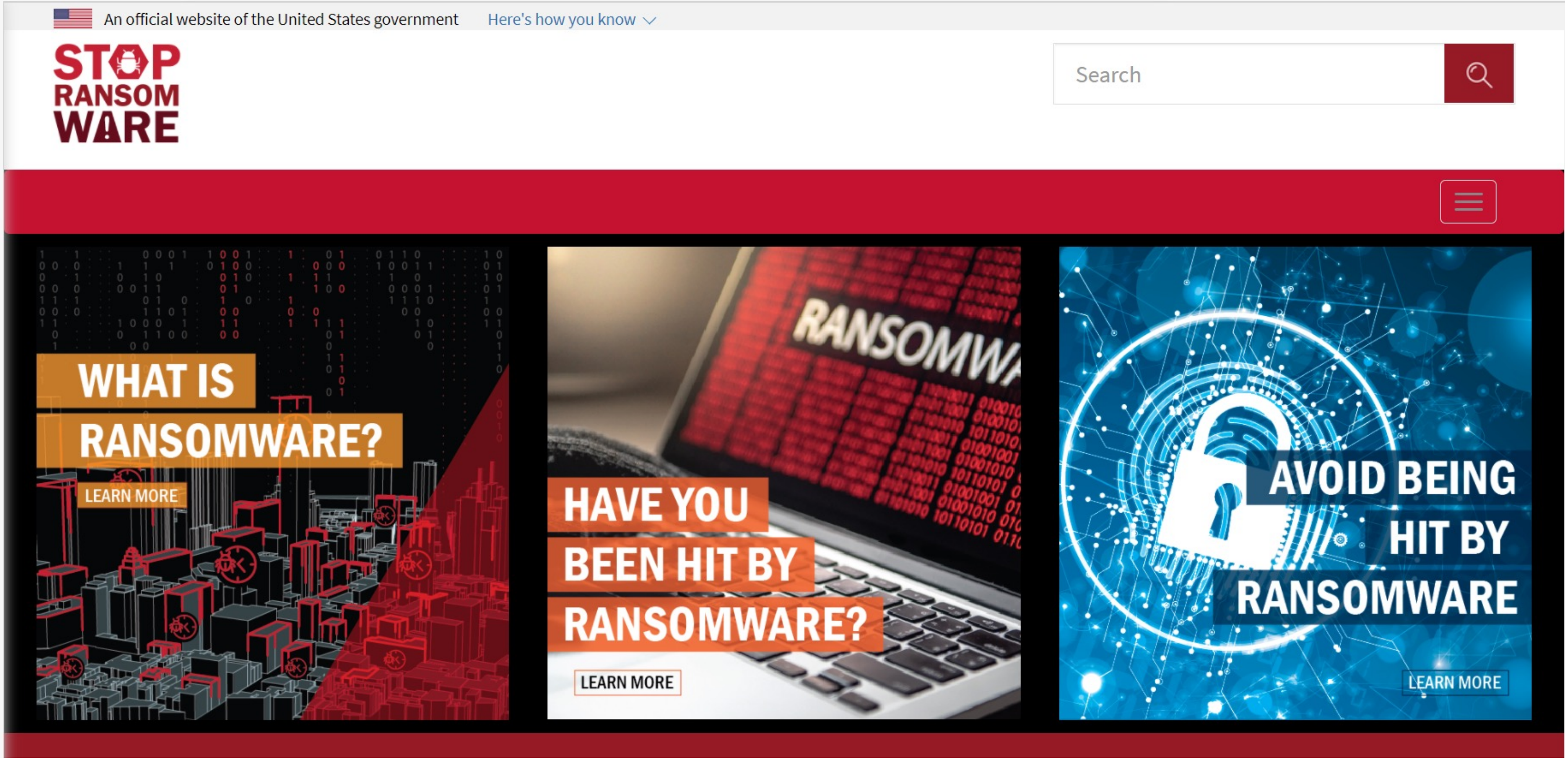
Security Awareness Training

Cyber Security Evaluation Tool: RRA

- **Ransomware Readiness Assessment:** The RRA is a self-assessment based on a tiered set of practices to help organizations better assess how well they are equipped to defend and recover from a ransomware incident.
- **Facilitated:** Self-Administered, undertaken independently
- **Benefits**:
- Helps organizations evaluate their cybersecurity posture, with respect to ransomware, against recognized standards and best practice recommendations in a systematic, disciplined, and repeatable manner.
- Guides asset owners and operators through a systematic process to evaluate their operational technology (OT) and information technology (IT) network security practices against the ransomware threat.
- Provides an analysis dashboard with graphs and tables that present the assessment results in both summary and detailed form.

INTRODUCING THE LATEST MODULE IN
CISA'S CYBER SECURITY EVALUATION TOOL:
RANSOMWARE
READINESS
ASSESSMENT
CSET

Federal Ransomware Website


An official website of the United States government
Here's how you know
STOP RANSOMWARE
Search
WHAT IS RANSOMWARE?
LEARN MORE
RANSOMWARE
HAVE YOU BEEN HIT BY RANSOMWARE?
LEARN MORE
AVOID BEING HIT BY RANSOMWARE
LEARN MORE

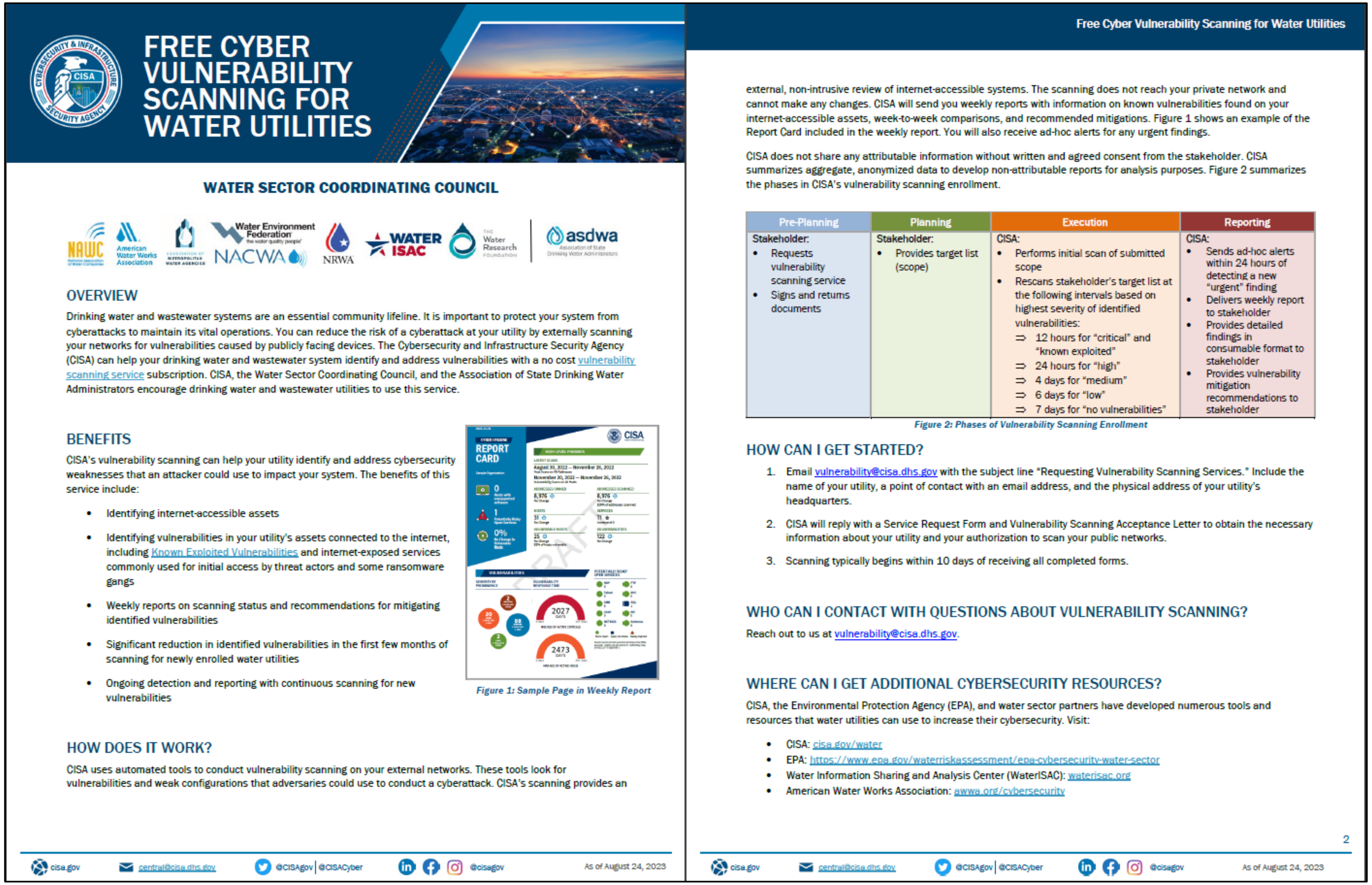
Visit StopRansomware.gov today!

Other CSET Self-Assessments

- External Dependencies Management (Strategic)
- Cyber Resilience Review (Strategic)
- Cyber Infrastructure Survey (Strategic/Technical)
- Incident Management Review (v.12)

CISA-FACILITATED ASSESSMENTS

Vulnerability Scanning



FREE CYBER VULNERABILITY SCANNING FOR WATER UTILITIES

WATER SECTOR COORDINATING COUNCIL

NAWC National Association of Water Companies · American Water Works Association · Association of Metropolitan Water Agencies · Water Environment Federation the water quality people · NACWA · NRWA · WATER ISAC · The Water Research Foundation · asdwa Association of State Drinking Water Administrators

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 external, non-intrusive review of internet-accessible systems. The scanning does not reach your private network and cannot make any changes. CISA will send you weekly reports with information on known vulnerabilities found on your internet-accessible assets, week-to-week comparisons, and recommended mitigations. Figure 1 shows an example of the Report Card included in the weekly report. You will also receive ad-hoc alerts for any urgent findings.

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

Free Cyber Vulnerability Scanning for Water Utilities

CISA does not share any attributable information without written and agreed consent from the stakeholder. CISA summarizes aggregate, anonymized data to develop non-attributable reports for analysis purposes. Figure 2 summarizes the phases in CISA's vulnerability scanning enrollment.

Pre-Planning	Planning	Execution	Reporting
Stakeholder: • Requests vulnerability scanning service • Signs and returns documents	Stakeholder: • Provides target list (scope)	CISA: • Performs initial scan of submitted scope • Rescans stakeholder's target list at the following intervals based on highest severity of identified vulnerabilities: ⇒ 12 hours for "critical" and "known exploited" ⇒ 24 hours for "high" ⇒ 4 days for "medium" ⇒ 6 days for "low" ⇒ 7 days for "no vulnerabilities"	CISA: • Sends ad-hoc alerts within 24 hours of detecting a new "urgent" finding • Delivers weekly report to stakeholder • Provides detailed findings in consumable format to stakeholder • Provides vulnerability mitigation recommendations to stakeholder

Figure 2: Phases of Vulnerability Scanning Enrollment

HOW CAN I GET STARTED?

1. Email vulnerability@cisa.dhs.gov with the subject line "Requesting Vulnerability Scanning Services." Include the name of your utility, a point of contact with an email address, and the physical address of your utility's headquarters.
2. CISA will reply with a Service Request Form and Vulnerability Scanning Acceptance Letter to obtain the necessary information about your utility and your authorization to scan your public networks.
3. Scanning typically begins within 10 days of receiving all completed forms.

WHO CAN I CONTACT WITH QUESTIONS ABOUT VULNERABILITY SCANNING?

Reach out to us at vulnerability@cisa.dhs.gov.

WHERE CAN I GET ADDITIONAL CYBERSECURITY RESOURCES?

CISA, the Environmental Protection Agency (EPA), and water sector partners have developed numerous tools and resources that water utilities can use to increase their cybersecurity. Visit:

- CISA: cisa.gov/water
- EPA: https://www.epa.gov/waterriskassessment/epa-cybersecurity-water-sector
- Water Information Sharing and Analysis Center (WaterISAC): waterisac.org
- American Water Works Association: awwa.org/cybersecurity

2

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

Vulnerability Scanning by CISA

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

Average time for a new CVE to become a KEV is **8 days**

Global average cost of a breach is **$4.45 million**

It can take businesses **9 months** to recover from a cyber attack

Businesses can lose **$5600** per minute of system downtime

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

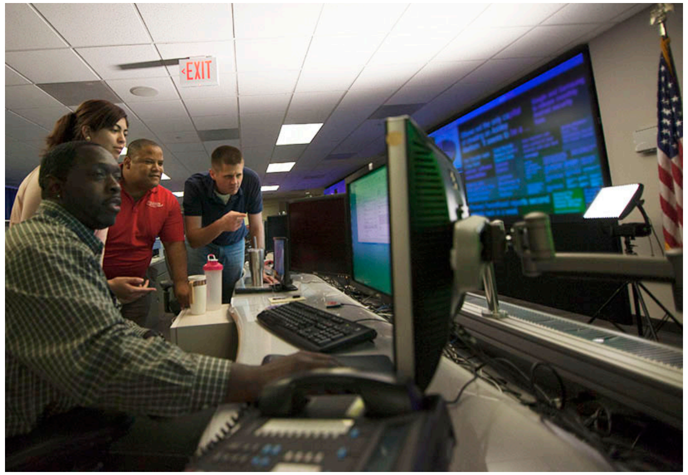
- **7,200+** current customers nationwide
- **Over 3 Million** vulnerabilities found and fixed
- On average a **40% reduction in risk and exposure** by newly enrolled customers in their first 12 months
- Most enrollees see improvements within the first **90 days**

GETTING STARTED

Email vulnerability@cisa.dhs.gov
Subject: "Requesting Vulnerability Scanning Services"

CISA-Facilitated Technical Assessments

- Web Application Scanning
- Remote Penetration Testing
- Validated Architecture Design Review
- Risk and Vulnerability Assessment



INCIDENT RESPONSE PLANNING

Incident Response Guide for Water & Wastewater Sector

This guide aims to enhance WWS Sector cybersecurity by:

1. Establishing clear guidance for reporting cyber incidents,
2. Connecting utilities with available cybersecurity resources, services, and no-cost trainings,
3. Empowering utilities to build a strong cybersecurity baseline to improve cyber resilience and cyber hygiene, and
4. Encouraging utilities to integrate into their local cyber communities.

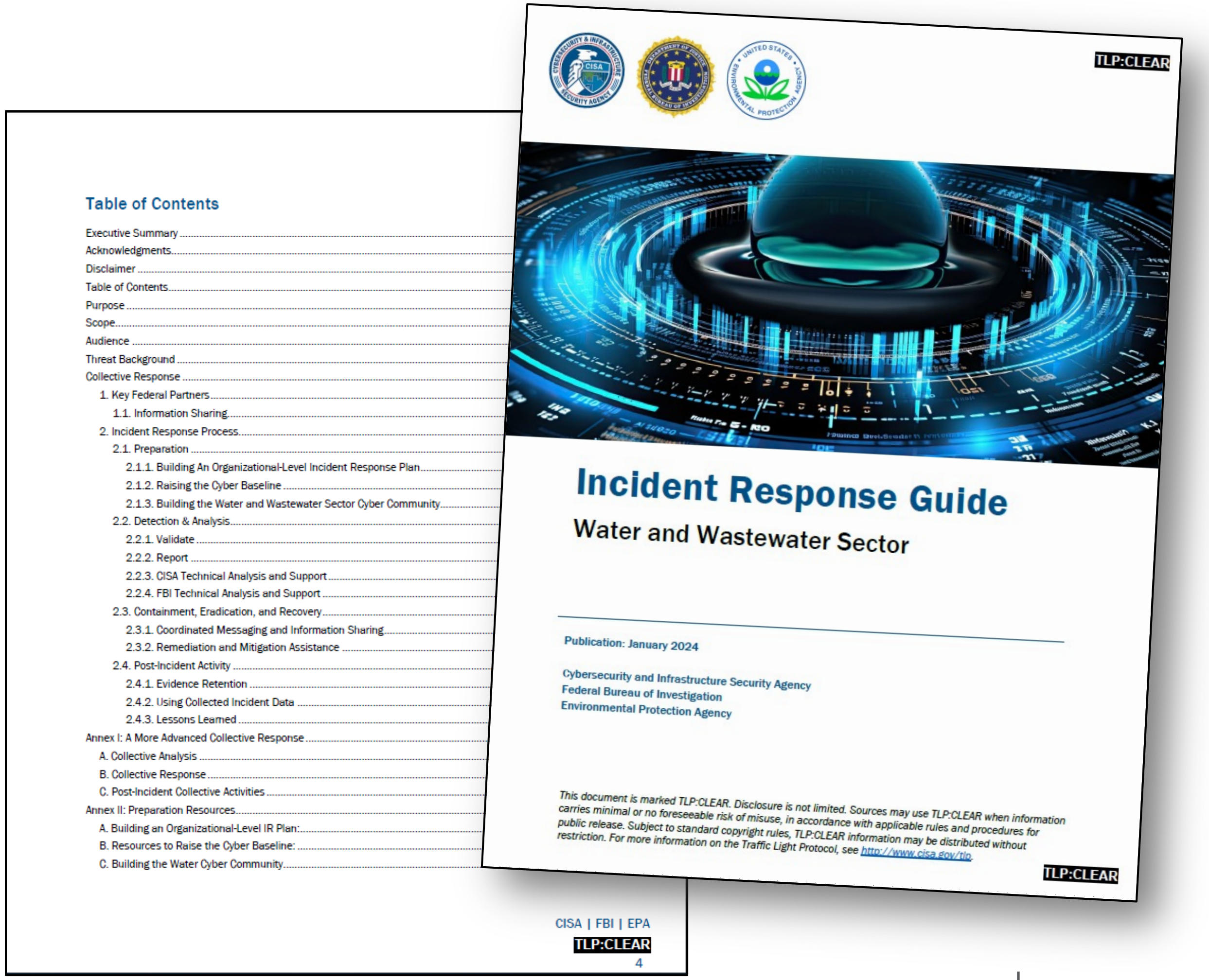


Table of Contents

CISA | FBI | EPA
TLP:CLEAR
4

TLP:CLEAR

Incident Response Guide

Water and Wastewater Sector

Publication: January 2024

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

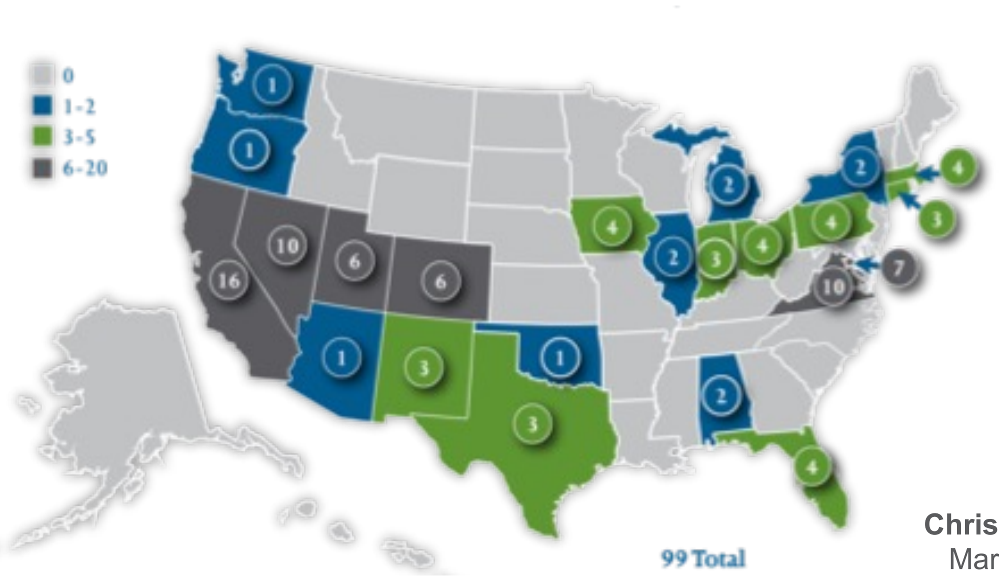
This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed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

TLP:CLEAR

Cyber Exercises and Planning

CISA's National Cyber Exercise and Planning Program develops, conducts, and evaluates cyber exercises and planning activities for state, local, tribal and territorial governments and public and private sector critical infrastructure organizations.

- Cyber Storm Exercise – DHS's flagship national-level biennial exercise
- Exercise Planning and Conduct
- Cyber Exercise Consulting and Subject Expertise Support
- Cyber Planning Support
- Off-the-Shelf Resources
- Exercise-In-A-Box



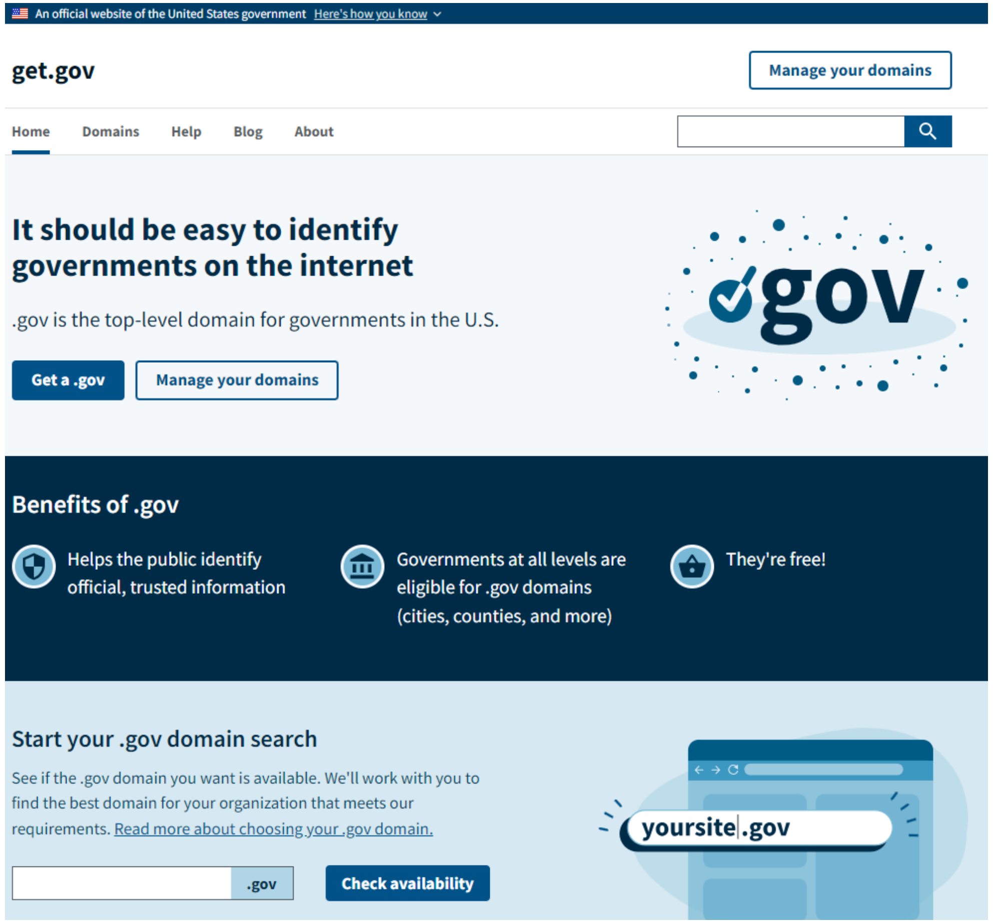
.gov

Registration re-opened January 31, 2024

Registration and Domains are FREE

Establishes Credibility

Visit get.gov today!



An official website of the United States government Here's how you know

get.gov

It should be easy to identify governments on the internet

.gov is the top-level domain for governments in the U.S.

Benefits of .gov

Helps the public identify official, trusted information

Governments at all levels are eligible for .gov domains (cities, counties, and more)

They're free!

Start your .gov domain search

See if the .gov domain you want is available. We'll work with you to find the best domain for your organization that meets our requirements. Read more about choosing your .gov domain.

4 Easy Ways to Stay Safe Online

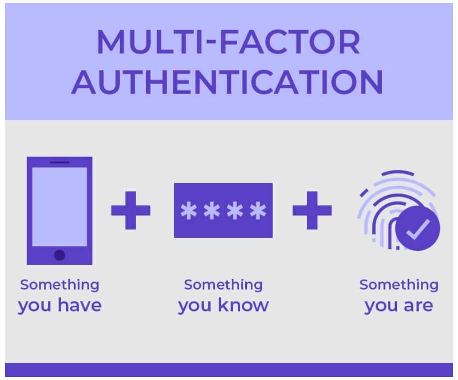
Strong coffee, good.
Strong passwords, better.
Learn more at cisa.gov/SecureOurWorld
SECURE OUR WORLD

Use Strong Passwords and a Password Manager

Turn on Multifactor Authentication

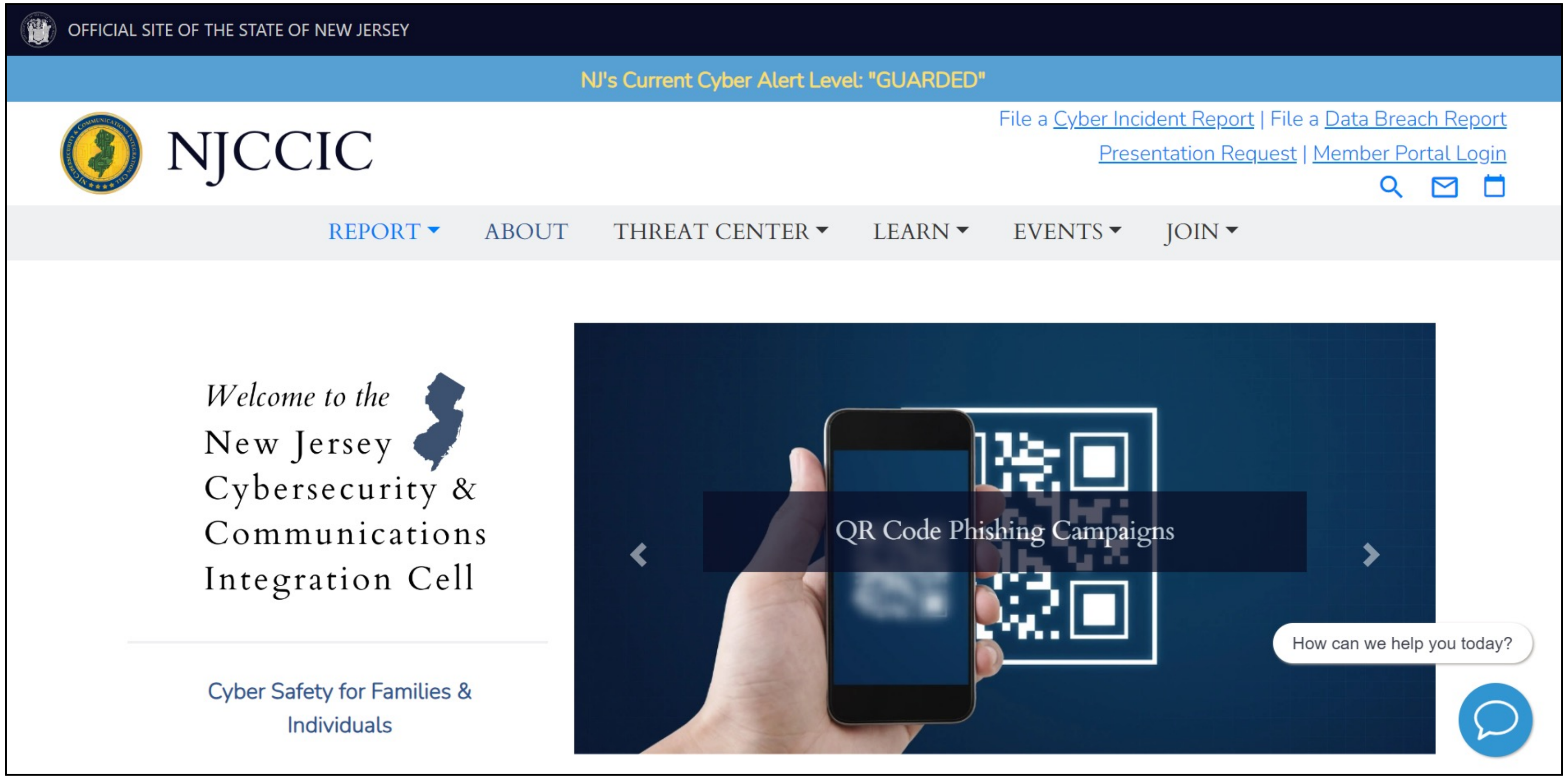
Recognize and Report Phishing Attacks

Update Your Software



Christopher Kay
March 19, 2024

Additional Information Sharing Opportunities



OFFICIAL SITE OF THE STATE OF NEW JERSEY

NJ's Current Cyber Alert Level: "GUARDED"

NJCCIC

File a Cyber Incident Report | File a Data Breach Report

Presentation Request | Member Portal Login

Welcome to the New Jersey Cybersecurity & Communications Integration Cell

Cyber Safety for Families & Individuals

QR Code Phishing Campaigns

How can we help you today?

www.cyber.nj.gov

Quick Review…

- CISA no-cost products and services for public & private sector organizations:

INTRODUCING THE LATEST MODULE IN CISA'S CYBER SECURITY EVALUATION TOOL:
RANSOMWARE READINESS ASSESSMENT
CSET

Christopher Kay

Cybersecurity Advisor

Region II (NY, **NJ**, PR, USVI)

christopher.kay@cisa.dhs.gov

CISA

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY