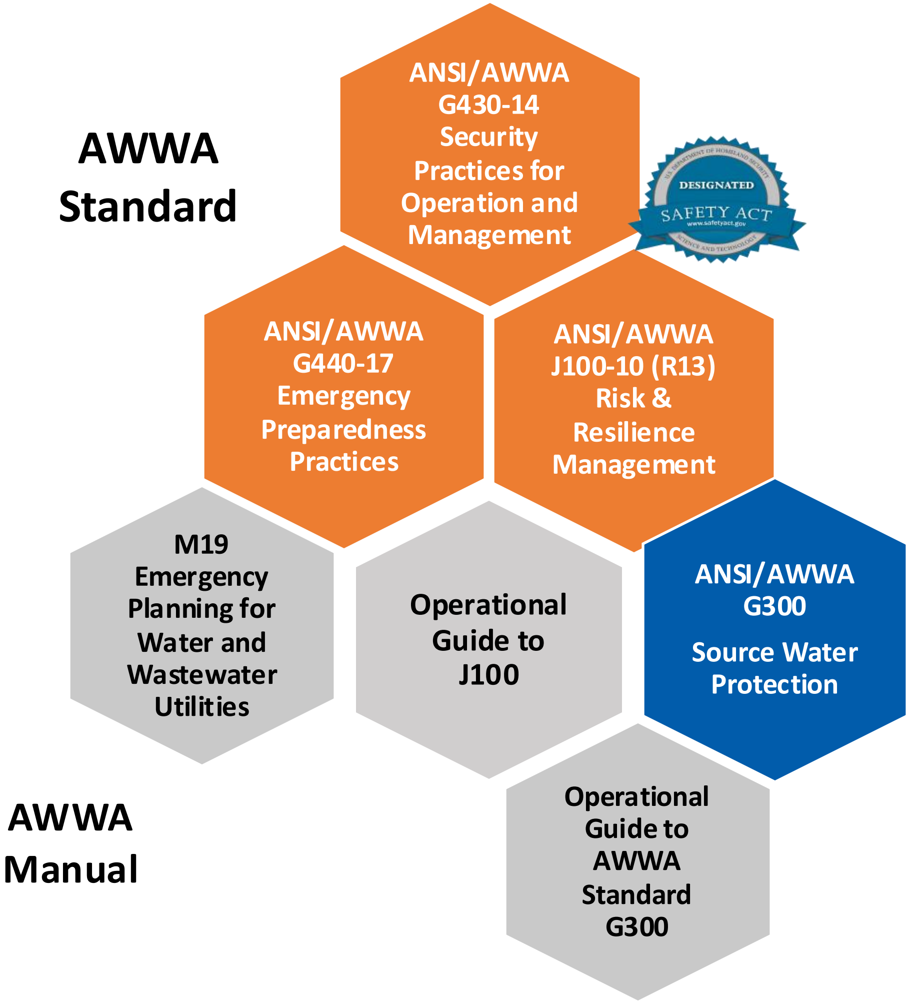
Cybersecurity in the Water Sector

Kevin Morley, PhD
American Water Works Association

American Water Works Association

AWWA RISK & RESILIENCE RESOURCE SUITE



AWWA Standard

ANSI/AWWA G430-14 Security Practices for Operation and Management

DESIGNATED SAFETY ACT

ANSI/AWWA G440-17 Emergency Preparedness Practices

ANSI/AWWA J100-10 (R13) Risk & Resilience Management

M19 Emergency Planning for Water and Wastewater Utilities

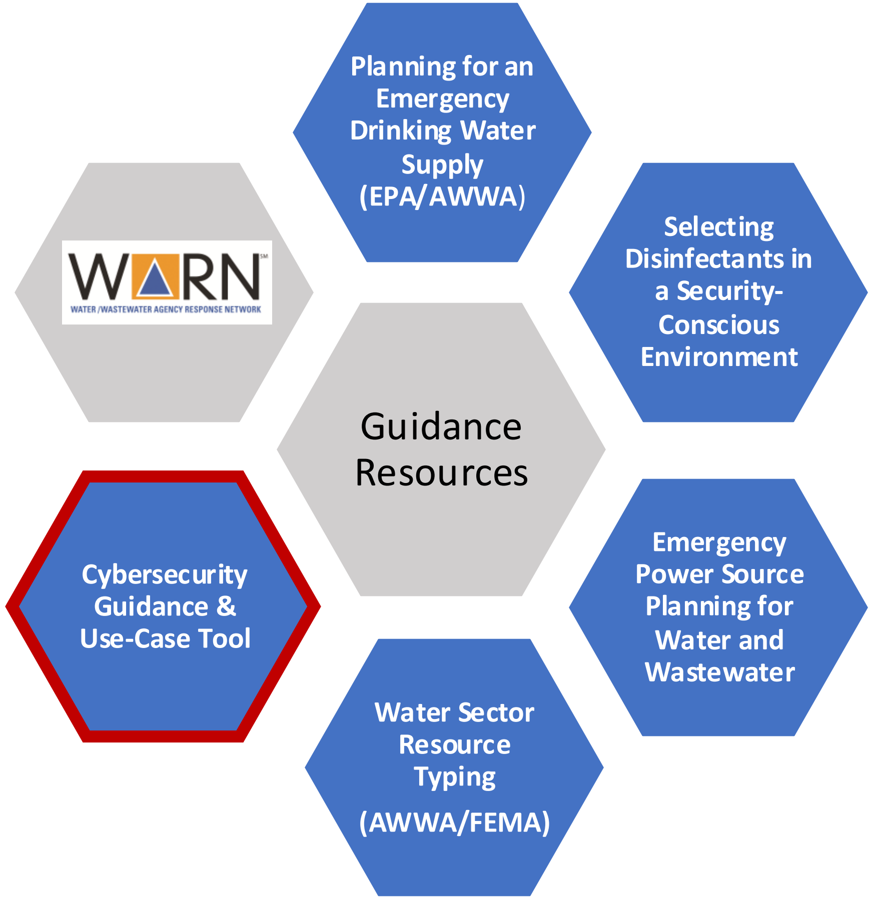
Operational Guide to J100

ANSI/AWWA G300

Source Water Protection

Operational Guide to AWWA Standard G300

AWWA Manual



WARN

WATER/WASTEWATER AGENCY RESPONSE NETWORK

Planning for an Emergency Drinking Water Supply (EPA/AWWA)

Selecting Disinfectants in a Security-Conscious Environment

Guidance Resources

Cybersecurity Guidance & Use-Case Tool

Emergency Power Source Planning for Water and Wastewater

Water Sector Resource Typing

(AWWA/FEMA)

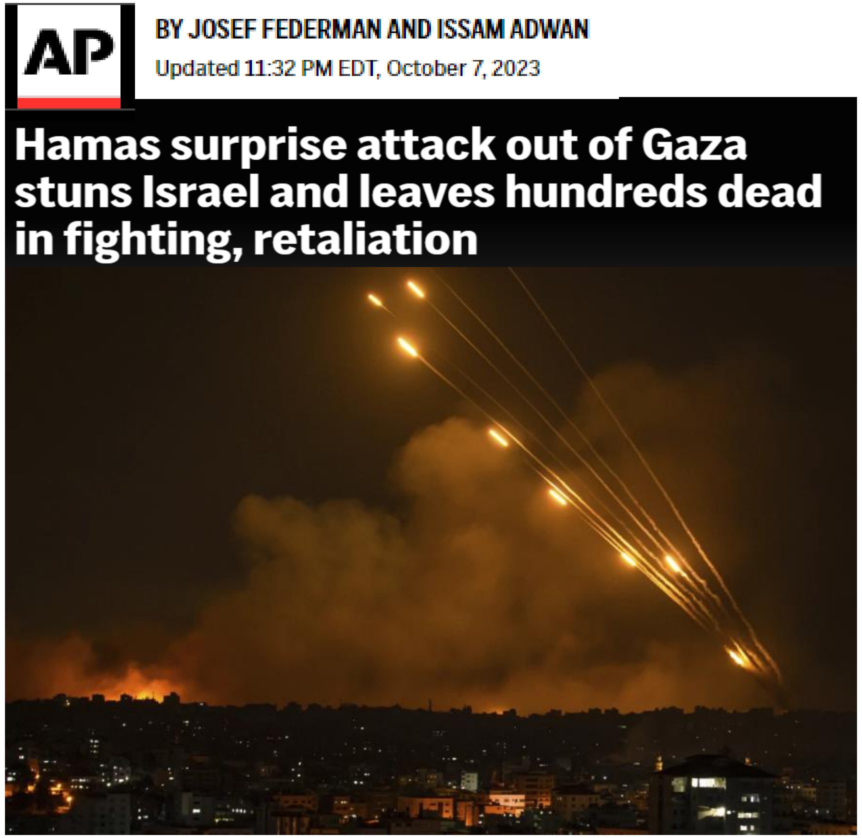
Looking Ahead

Awareness

Analysis

Action

AWARENESS – THE THREAT



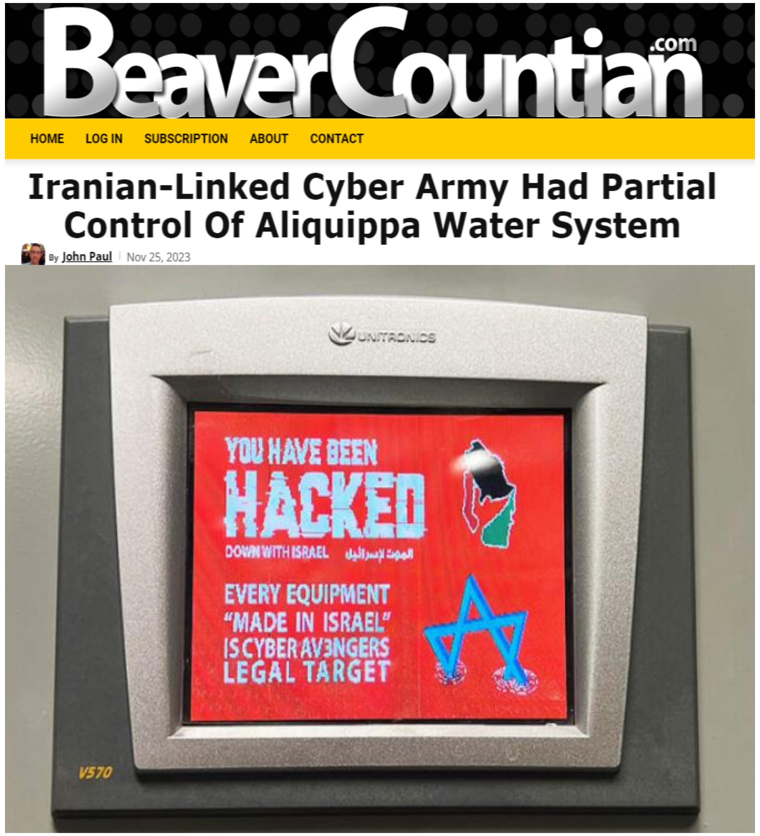
AP

BY JOSEF FEDERMAN AND ISSAM ADWAN

Updated 11:32 PM EDT, October 7, 2023

Hamas surprise attack out of Gaza stuns Israel and leaves hundreds dead in fighting, retaliation

AP Photo/Fatima Shbair



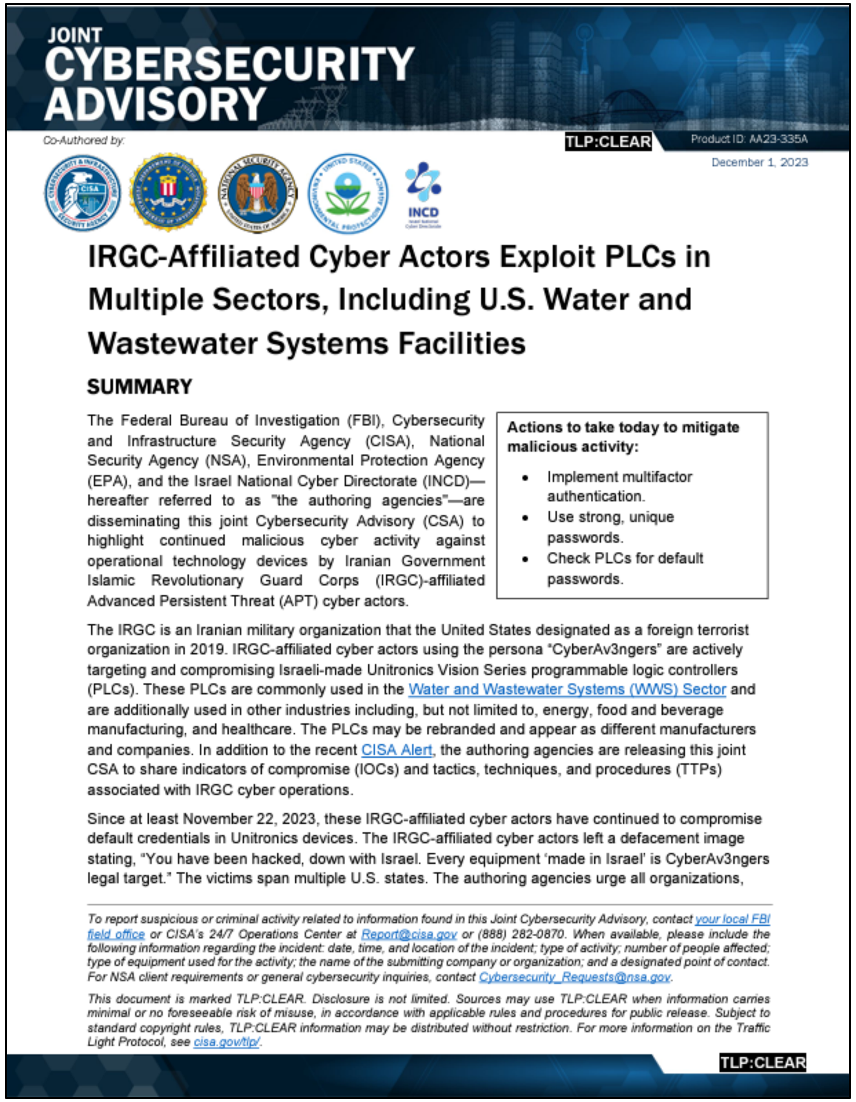
BeaverCountian.com

HOME LOG IN SUBSCRIPTION ABOUT CONTACT

Iranian-Linked Cyber Army Had Partial Control Of Aliquippa Water System

By John Paul | Nov 25, 2023

AWARENESS – THE THREAT



JOINT CYBERSECURITY ADVISORY

Co-Authored by:

TLP:CLEAR

Product ID: AA23-335A

December 1, 2023

IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities

SUMMARY

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Environmental Protection Agency (EPA), and the Israel National Cyber Directorate (INCD)—hereafter referred to as "the authoring agencies"—are disseminating this joint Cybersecurity Advisory (CSA) to highlight continued malicious cyber activity against operational technology devices by Iranian Government Islamic Revolutionary Guard Corps (IRGC)-affiliated Advanced Persistent Threat (APT) cyber actors.

Actions to take today to mitigate malicious activity:

- Implement multifactor authentication.
- Use strong, unique passwords.
- Check PLCs for default passwords.

The IRGC is an Iranian military organization that the United States designated as a foreign terrorist organization in 2019. IRGC-affiliated cyber actors using the persona "CyberAv3ngers" are actively targeting and compromising Israeli-made Unitronics Vision Series programmable logic controllers (PLCs). These PLCs are commonly used in the Water and Wastewater Systems (WWS) Sector and are additionally used in other industries including, but not limited to, energy, food and beverage manufacturing, and healthcare. The PLCs may be rebranded and appear as different manufacturers and companies. In addition to the recent CISA Alert, the authoring agencies are releasing this joint CSA to share indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) associated with IRGC cyber operations.

Since at least November 22, 2023, these IRGC-affiliated cyber actors have continued to compromise default credentials in Unitronics devices. The IRGC-affiliated cyber actors left a defacement image stating, "You have been hacked, down with Israel. Every equipment 'made in Israel' is CyberAv3ngers legal target." The victims span multiple U.S. states. The authoring agencies urge all organizations,

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office or CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. For NSA client requirements or general cybersecurity inquiries, contact Cybersecurity_Requests@nsa.gov.

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

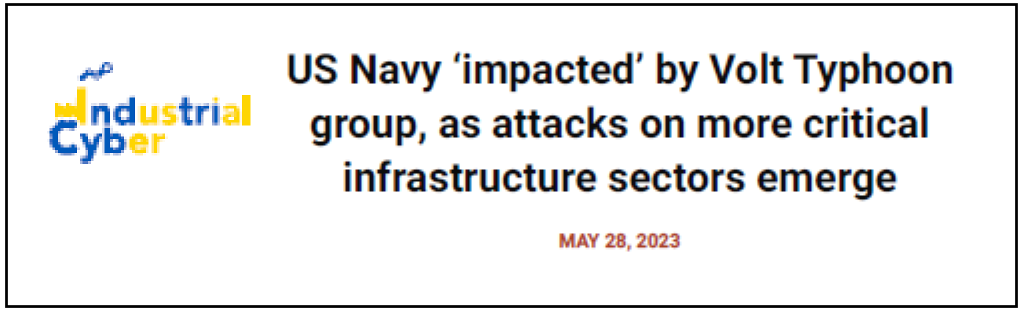
December 1, 2023

Actions to take today:

- Change default passwords on PLCs & HMIs.
- Ensure PLCs are not on public-facing internet connections.
- Use strong, unique passwords.
- Implement multifactor authentication.

https://www.cisa.gov/sites/default/files/2023-12/aa23-335a-irgc-affiliated-cyber-actors-exploit-plcs-in-multiple-sectors-1.pdf

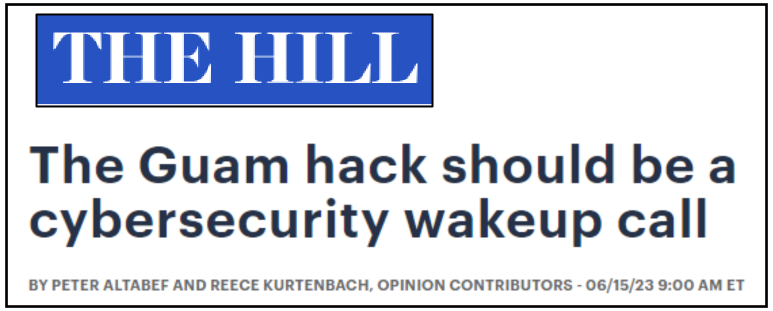
AWARENESS – THE THREAT



Industrial Cyber

US Navy 'impacted' by Volt Typhoon group, as attacks on more critical infrastructure sectors emerge

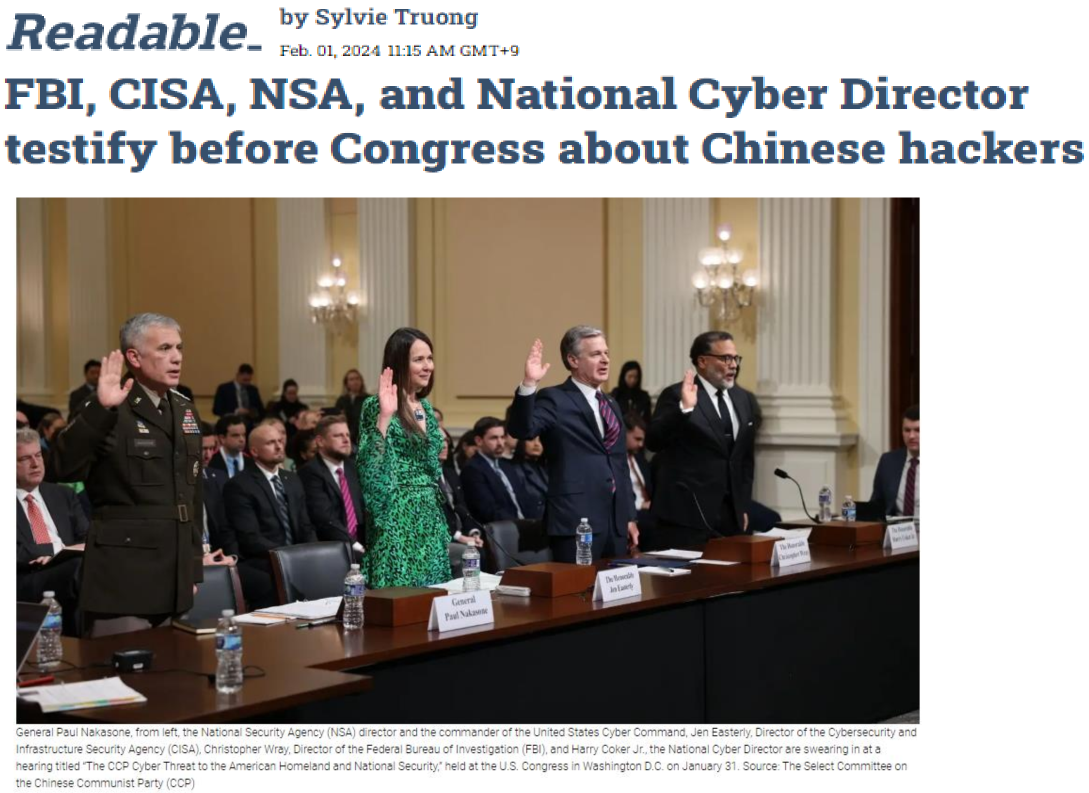
MAY 28, 2023



THE HILL

The Guam hack should be a cybersecurity wakeup call

BY PETER ALTABEF AND REECE KURTENBACH, OPINION CONTRIBUTORS - 06/15/23 9:00 AM ET



Readable by Sylvie Truong

Feb. 01, 2024 11:15 AM GMT+9

FBI, CISA, NSA, and National Cyber Director testify before Congress about Chinese hackers

General Paul Nakasone, from left, the National Security Agency (NSA) director and the commander of the United States Cyber Command, Jen Easterly, Director of the Cybersecurity and Infrastructure Security Agency (CISA), Christopher Wray, Director of the Federal Bureau of Investigation (FBI), and Harry Coker Jr., the National Cyber Director are swearing in at a hearing titled "The CCP Cyber Threat to the American Homeland and National Security," held at the U.S. Congress in Washington D.C. on January 31. Source: The Select Committee on the Chinese Communist Party (CCP)

AWARENESS – THE THREAT

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

February 7, 2024

Actions to take today:

- Apply patches for internet-facing systems. Prioritize patching critical vulnerabilities in appliances known to be frequently exploited by Volt Typhoon.

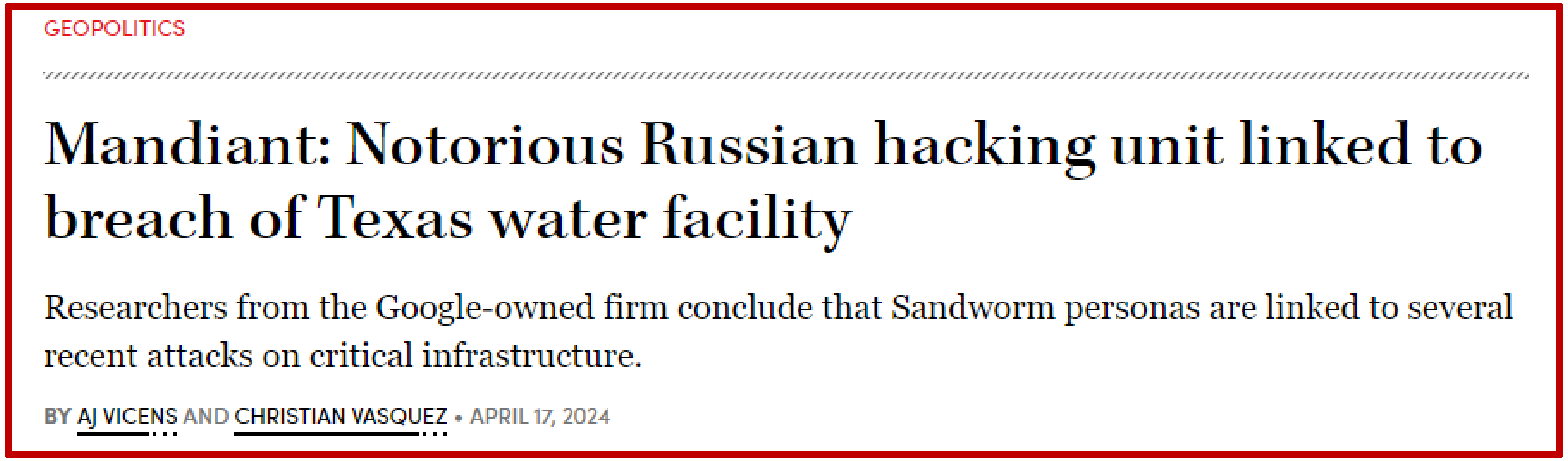
- Implement phishing-resistant MFA.

- Ensure logging is turned on for application, access, and security logs and store logs in a central system.

- Plan “end of life” for technology beyond manufacturer’s supported lifecycle.

https://www.cisa.gov/sites/default/files/2024-03/aa24-038a_csa_prc_state_sponsored_actors_compromise_us_critical_infrastructure_3.pdf

AWARENESS – THE THREAT

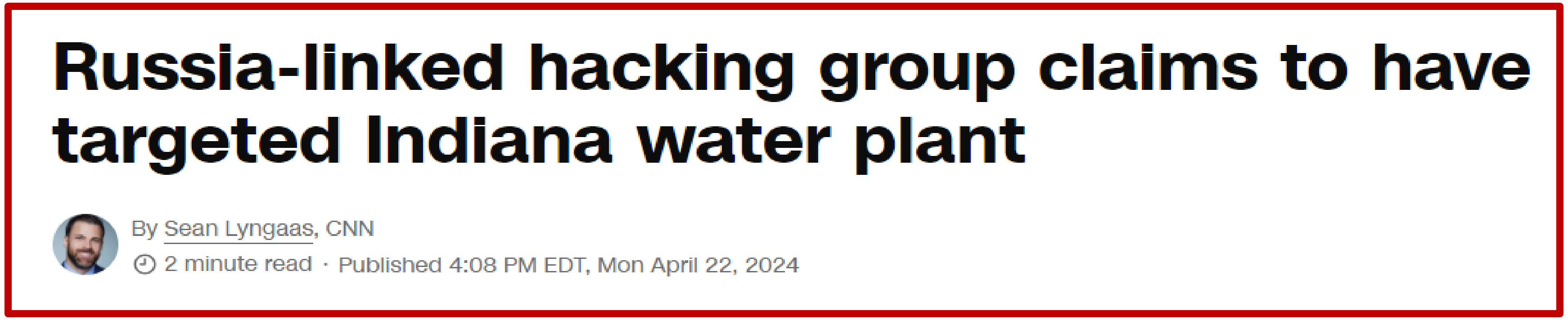


GEOPOLITICS

Mandiant: Notorious Russian hacking unit linked to breach of Texas water facility

Researchers from the Google-owned firm conclude that Sandworm personas are linked to several recent attacks on critical infrastructure.

BY AJ VICENS AND CHRISTIAN VASQUEZ • APRIL 17, 2024

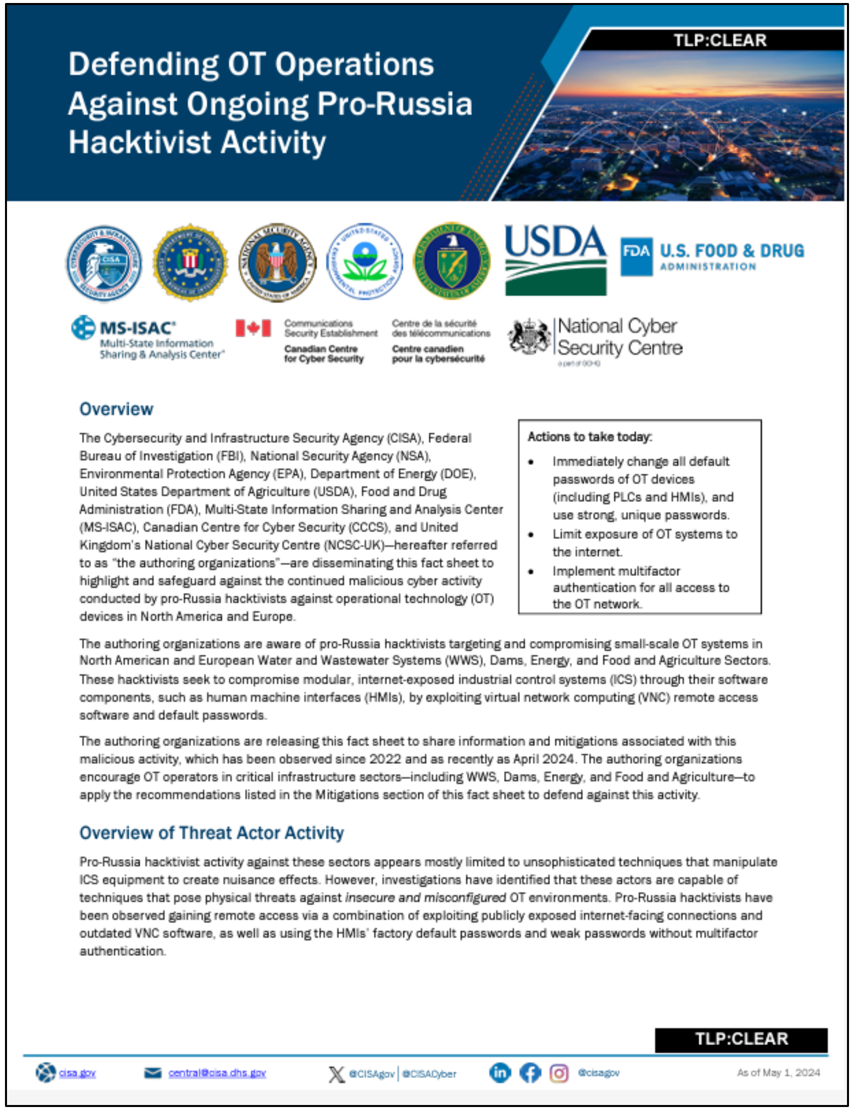


Russia-linked hacking group claims to have targeted Indiana water plant

By Sean Lyngaas, CNN

2 minute read · Published 4:08 PM EDT, Mon April 22, 2024

AWARENESS – THE THREAT



TLP:CLEAR

Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity

MS-ISAC Multi-State Information Sharing & Analysis Center

Communications Security Establishment Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications Centre canadien pour la cybersécurité

National Cyber Security Centre

Overview

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), National Security Agency (NSA), Environmental Protection Agency (EPA), Department of Energy (DOE), United States Department of Agriculture (USDA), Food and Drug Administration (FDA), Multi-State Information Sharing and Analysis Center (MS-ISAC), Canadian Centre for Cyber Security (CCCS), and United Kingdom's National Cyber Security Centre (NCSC-UK)—hereafter referred to as "the authoring organizations"—are disseminating this fact sheet to highlight and safeguard against the continued malicious cyber activity conducted by pro-Russia hacktivists against operational technology (OT) devices in North America and Europe.

Actions to take today:

- Immediately change all default passwords of OT devices (including PLCs and HMIs), and use strong, unique passwords.
- Limit exposure of OT systems to the internet.
- Implement multifactor authentication for all access to the OT network.

The authoring organizations are aware of pro-Russia hacktivists targeting and compromising small-scale OT systems in North American and European Water and Wastewater Systems (WWS), Dams, Energy, and Food and Agriculture Sectors. These hacktivists seek to compromise modular, internet-exposed industrial control systems (ICS) through their software components, such as human machine interfaces (HMIs), by exploiting virtual network computing (VNC) remote access software and default passwords.

The authoring organizations are releasing this fact sheet to share information and mitigations associated with this malicious activity, which has been observed since 2022 and as recently as April 2024. The authoring organizations encourage OT operators in critical infrastructure sectors—including WWS, Dams, Energy, and Food and Agriculture—to apply the recommendations listed in the Mitigations section of this fact sheet to defend against this activity.

Overview of Threat Actor Activity

Pro-Russia hacktivist activity against these sectors appears mostly limited to unsophisticated techniques that manipulate ICS equipment to create nuisance effects. However, investigations have identified that these actors are capable of techniques that pose physical threats against *insecure and misconfigured* OT environments. Pro-Russia hacktivists have been observed gaining remote access via a combination of exploiting publicly exposed internet-facing connections and outdated VNC software, as well as using the HMIs' factory default passwords and weak passwords without multifactor authentication.

TLP:CLEAR

cisa.gov central@cisa.dhs.gov @CISAgov | @CISACyber @cisagov As of May 1, 2024

May 1, 2024

Actions to take today:

1. Immediately change all default passwords of OT devices (including PLCs and HMIs), and use strong, unique passwords.

2. Limit exposure of OT systems to the internet.

3. Implement multifactor authentication for all access to the OT network.

https://www.cisa.gov/news-events/alerts/2024/05/01/cisa-and-partners-release-fact-sheet-defending-ot-operations-against-ongoing-pro-russia-hacktivist

Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems, November 2023–April 2024

Iran-affiliated and pro-Russia cyber actors gained access to and in some cases have manipulated critical US industrial control systems (ICS) in the food and agriculture, healthcare, and water and wastewater sectors in late 2023 and 2024. These attacks highlight a potential public safety threat and an avenue for malicious cyber actors to cause physical damage and deny critical services. Outdated software, poor password security, the use of default credentials, and limited resources for system updates render ICS devices vulnerable to compromise, as they are commonly connected to corporate IT networks and increasingly to the Internet. Many operators face numerous competing priorities, such as physical facilities operations and maintenance, which further constrains the time and resources that operators can dedicate to cybersecurity practices. Furthermore, the limited number of ICS vendors, wide availability of product configurations, and operational commonalities across the water sector make it easier for cyber actors to compromise vulnerable systems.

IRGC-affiliated "Cyber Av3ngers" compromise Unitronics programmable logic controllers (PLCs)

In November 2023, IRGC-affiliated actors operating under the Cyber Av3ngers persona gained access to the Israeli-made Unitronics Series ICS PLCs in multiple US entities, mostly water and wastewater systems, and defaced the PLCs' touch screens with an anti-Israel message. In response to the defacement, a few of the water-sector victims briefly shut down their systems and switched to manual operations.

Pro-Russia hacktivist compromised several water plants and claimed to compromise two dairies

A pro-Russia hacktivist remotely manipulated control systems within five water and wastewater systems and two dairies. The actors have typically accessed the ICS components via control interfaces with public-facing IP addresses.

- On 20 and 24 April 2024, the group posted videos showing an attacker remotely manipulating settings on human-machine interfaces (HMIs) within two US wastewater systems and one purported US energy company.
- On 18 January 2024, the group accessed control systems at two Texas water facilities and tampered with their water pumps and alarms, causing water to run past designated shutoff levels and overfill storage tanks.
- On 23 and 27 November 2023, the group also claimed on its public Telegram channel that it had attacked two US dairy systems.

REPORTED CYBER ATTACKS ON US ICS, 23 NOVEMBER 2023 THROUGH 22 APRIL 2024

CYBER ACTORS

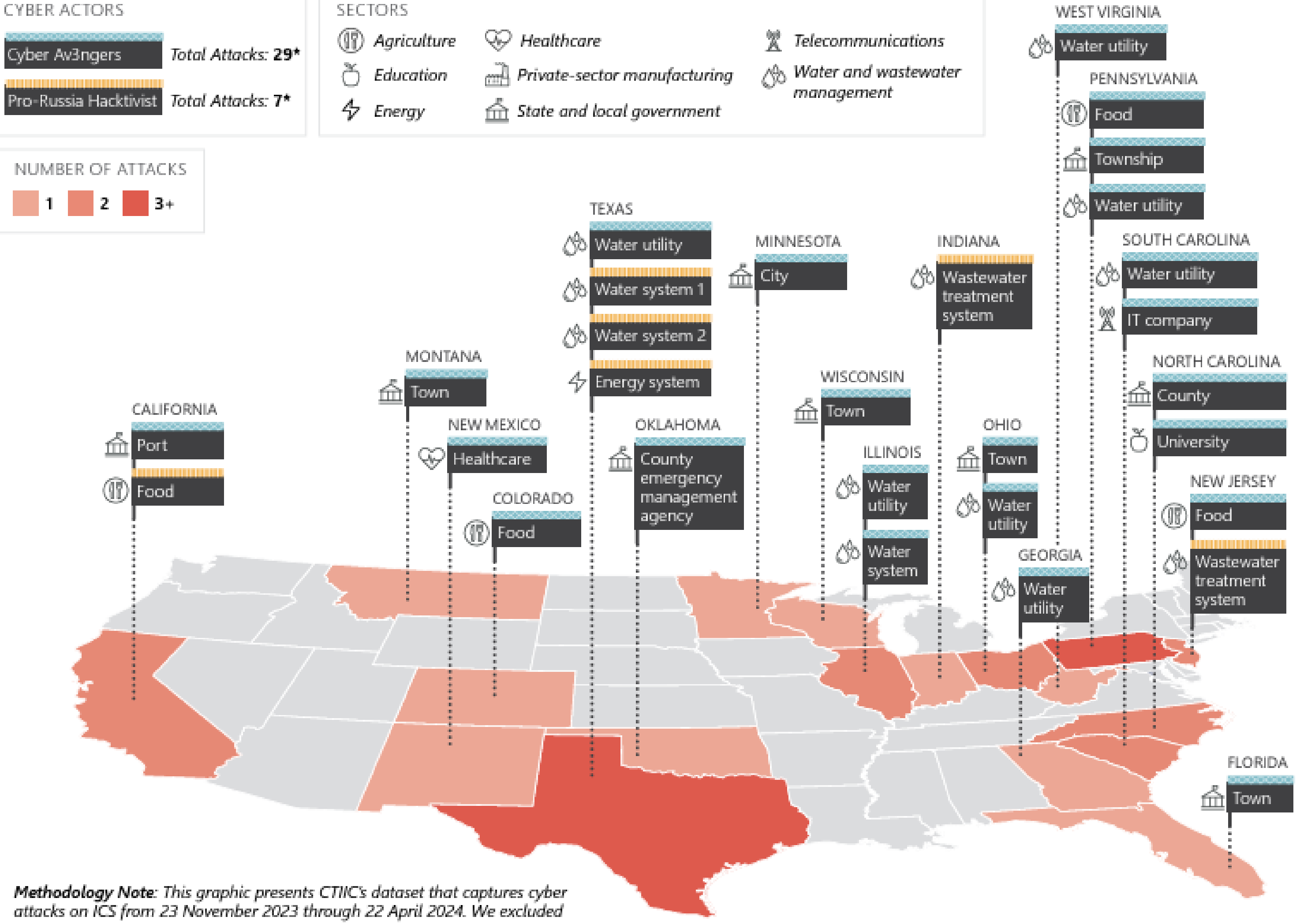
Cyber Av3ngers	*Total Attacks:* **29***
Pro-Russia Hacktivist	*Total Attacks:* **7***

SECTORS

Agriculture · *Education* · *Energy* · *Healthcare* · *Private-sector manufacturing* · *State and local government* · *Telecommunications* · *Water and wastewater management*

NUMBER OF ATTACKS

🟥 1 🟥 2 🟥 3+



***Methodology Note**: This graphic presents CTIIC's dataset that captures cyber attacks on ICS from 23 November 2023 through 22 April 2024. We excluded ransomware attacks on critical infrastructure entities.*

*Including seven attacks at additional US locations.

FY23 RVA Results

MITRE ATT&CK™ TACTICS AND TECHNIQUES

Initial Access

Threat actors attempt to obtain unauthorized initial access into a victim's network. Actors use techniques, such as Valid Accounts T1078 or Spear Phishing Link T1566.002s, to gain this access. After obtaining initial access, actors can then execute other techniques to move about the network.

Mitigations

Organizations can mitigate the risks associated with this technique by adhering to the following CPGs:

CPG 1.E Mitigating Known Vulnerabilities CPG 2.A Changing Default Passwords

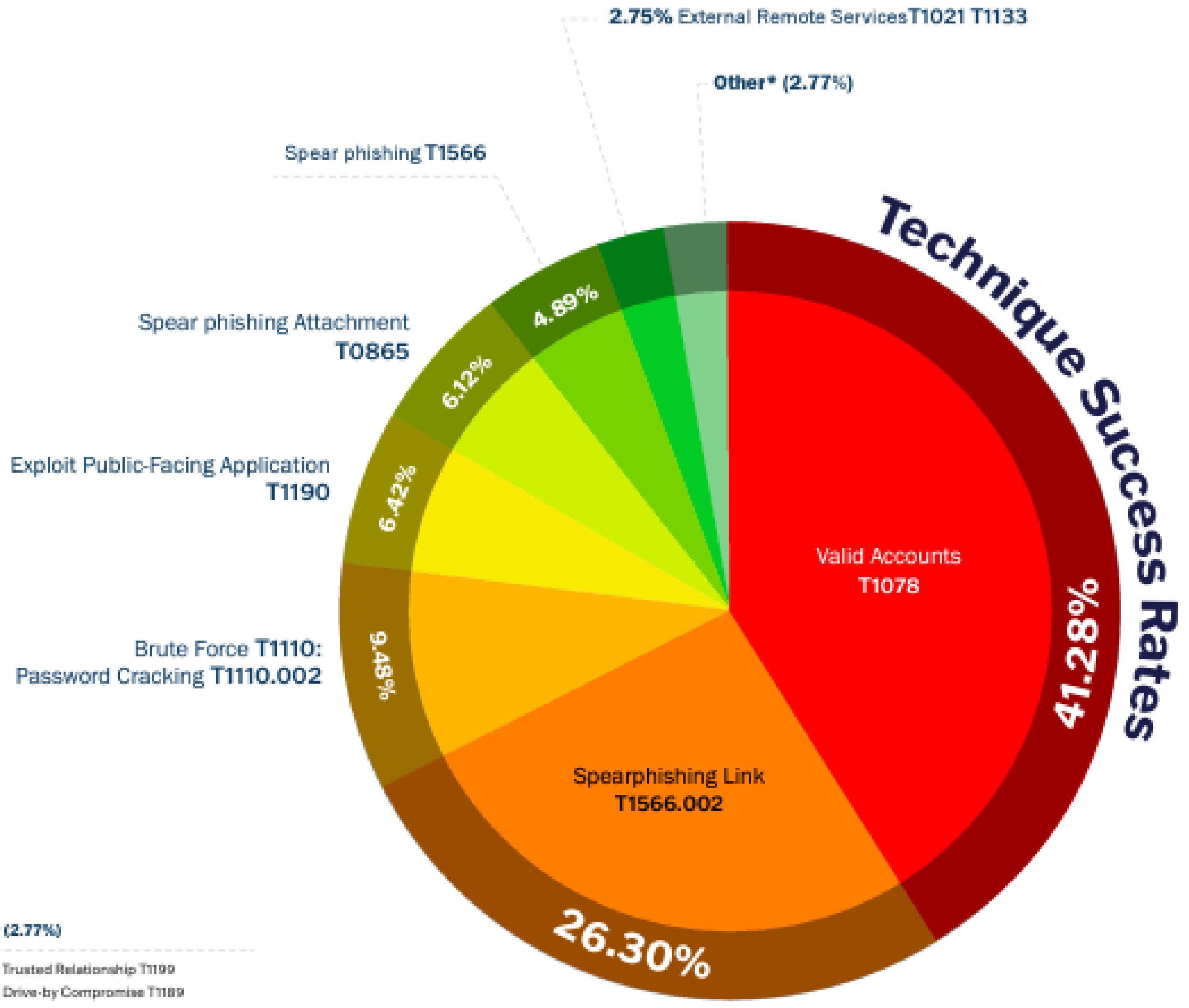
CPG 2.H Phishing-Resistant Multifactor Authentication CPG 2.M Email Security

CPG 2.N Disable Macros by Default

CPG 2.W No Exploitable Services on the Internet

ATT&CK®

This advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) and Pre-ATT&CK frameworks. See the ATT&CK for Enterprise and Pre-ATT&CK frameworks for referenced threat actor techniques. For more information about CISA assessment services, please visit **cisa.gov**



*Other (2.77%)

0.92%	Trusted Relationship T1199
0.92%	Drive-by Compromise T1189
0.31%	Hardware Additions T1200
0.31%	Replication Through Removable Media
0.31%	Process Injection T1631 T1055

Staying informed about the Threats

America's Cyber Defense Agency

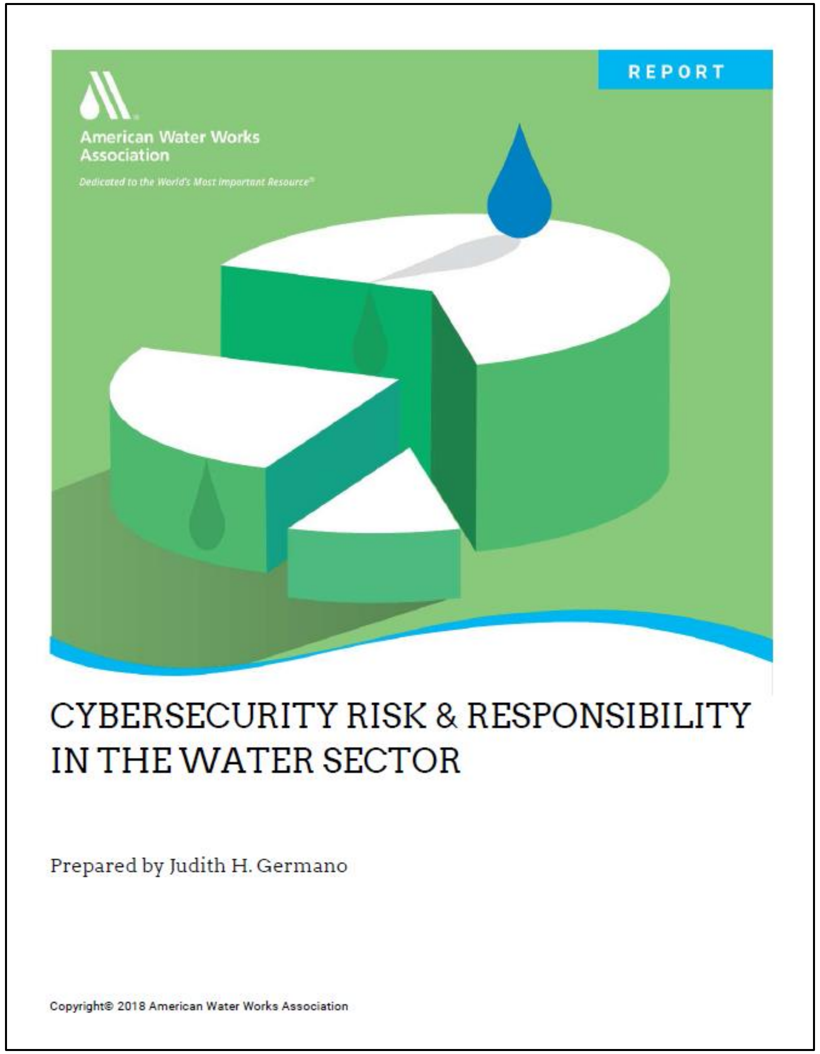
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

https://www.cisa.gov/news-events/cybersecurity-advisories

WATER ISAC

https://www.waterisac.org

Cybersecurity Risk & Responsibility



REPORT

American Water Works Association

Dedicated to the World's Most Important Resource®

CYBERSECURITY RISK & RESPONSIBILITY IN THE WATER SECTOR

Prepared by Judith H. Germano

Copyright® 2018 American Water Works Association

- **Cyber Threats are *Foreseeable***
- Implement Best Practices
- Demonstrate Due Diligence
- Insurance provides some risk transfer
- Sovereign Immunity is not option
- ***Fiduciary Responsibility***

AWARENESS - POLICY

AWIA §2013 (SDWA §1433) Round 2

Community Water System (pop. served)*‡	Certify Risk & Resilience Assessment (RRA) by:	Certify ERP within 6 months of RRA, but not later than:
≥ 100,000	March 31, 2025	September 30, 2025
50,000 – 99,999	December 31, 2025	June 30, 2026
3,300 – 49,999	June 30, 2026	December 30, 2026

*** Wholesalers use population of all systems served**

‡ Population as of March 31, 2024

AWARENESS - POLICY

EPA Enforcement Alert – May 20, 2024

EPA Region Performing Inspections

- Validate utility certification of RRA and ERP…must show physical copy
- Are all required elements included?
- Focused seems to be Tier 1 (100K+)
- Part of broader EPA Enforcement initiative targeting

Findings

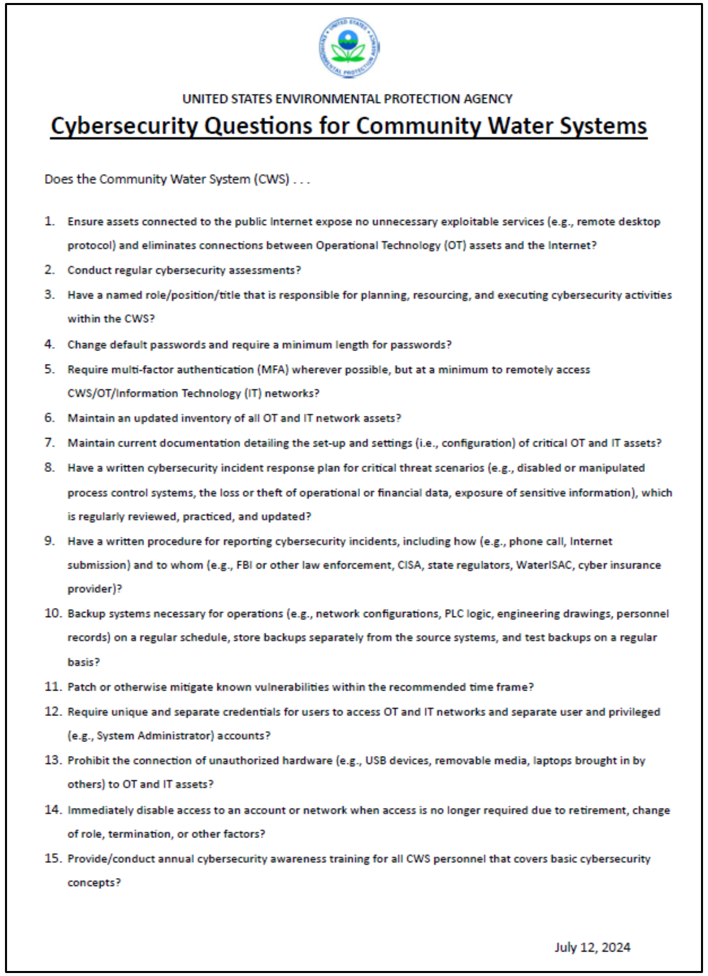
- EPA inspected ~40 systems Sept 2023-April 2024 found 70%
- *"do not fully comply"*
- Administrative Orders have stated that the RRA or ERP "*did not include sufficient details*"

AWARENESS - POLICY

EPA Cybersecurity Enforcement Focus

Focus is Observation of 15 Controls

- Based on subset of CISA Cybersecurity Performance Goals (CPGs)
- Guidance is derived from the withdrawn 2023 Sanitary Survey Cyber Rule
- List is included in 2 EPA sources:
  - **Evaluating Cybersecurity During Public Water System Sanitary Surveys** (817-B-23-001)
  - **Small System RRA Checklist for Drinking Water Utilities - use for compliance with SDWA 1433/AWIA 2013 (pdf)** (817-B-20-001, see Table 11)



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY

Cybersecurity Questions for Community Water Systems

Does the Community Water System (CWS) . . .

1. Ensure assets connected to the public Internet expose no unnecessary exploitable services (e.g., remote desktop protocol) and eliminates connections between Operational Technology (OT) assets and the Internet?
2. Conduct regular cybersecurity assessments?
3. Have a named role/position/title that is responsible for planning, resourcing, and executing cybersecurity activities within the CWS?
4. Change default passwords and require a minimum length for passwords?
5. Require multi-factor authentication (MFA) wherever possible, but at a minimum to remotely access CWS/OT/Information Technology (IT) networks?
6. Maintain an updated inventory of all OT and IT network assets?
7. Maintain current documentation detailing the set-up and settings (i.e., configuration) of critical OT and IT assets?
8. Have a written cybersecurity incident response plan for critical threat scenarios (e.g., disabled or manipulated process control systems, the loss or theft of operational or financial data, exposure of sensitive information), which is regularly reviewed, practiced, and updated?
9. Have a written procedure for reporting cybersecurity incidents, including how (e.g., phone call, Internet submission) and to whom (e.g., FBI or other law enforcement, CISA, state regulators, WaterISAC, cyber insurance provider)?
10. Backup systems necessary for operations (e.g., network configurations, PLC logic, engineering drawings, personnel records) on a regular schedule, store backups separately from the source systems, and test backups on a regular basis?
11. Patch or otherwise mitigate known vulnerabilities within the recommended time frame?
12. Require unique and separate credentials for users to access OT and IT networks and separate user and privileged (e.g., System Administrator) accounts?
13. Prohibit the connection of unauthorized hardware (e.g., USB devices, removable media, laptops brought in by others) to OT and IT assets?
14. Immediately disable access to an account or network when access is no longer required due to retirement, change of role, termination, or other factors?
15. Provide/conduct annual cybersecurity awareness training for all CWS personnel that covers basic cybersecurity concepts?

July 12, 2024

AWARENESS - POLICY

Change in Leadership means New Direction

- **EO 14179: Removing Barriers To American Leadership In Artificial Intelligence**
  - Develop *AI Action Plan* within 180 days (July 22, 2025)
  - Revokes EO 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

- **All National Security Memoranda (NSMs) are under review, including.**
  - NSM-5: Improving Cybersecurity for Critical Infrastructure Control Systems
    - Triggered creation of Cybersecurity Security Performance Goals (CPGs)

  - NSM-22: Critical Infrastructure Security and Resilience (replaced PPD-21)

Legislative Action

- **H.R. 2494**, Establish a Water Risk and Resilience Organization (WRRO) to develop cybersecurity requirements for the water sector

- **H.R.2109/S.1018**, Cybersecurity for Rural Water Systems Act

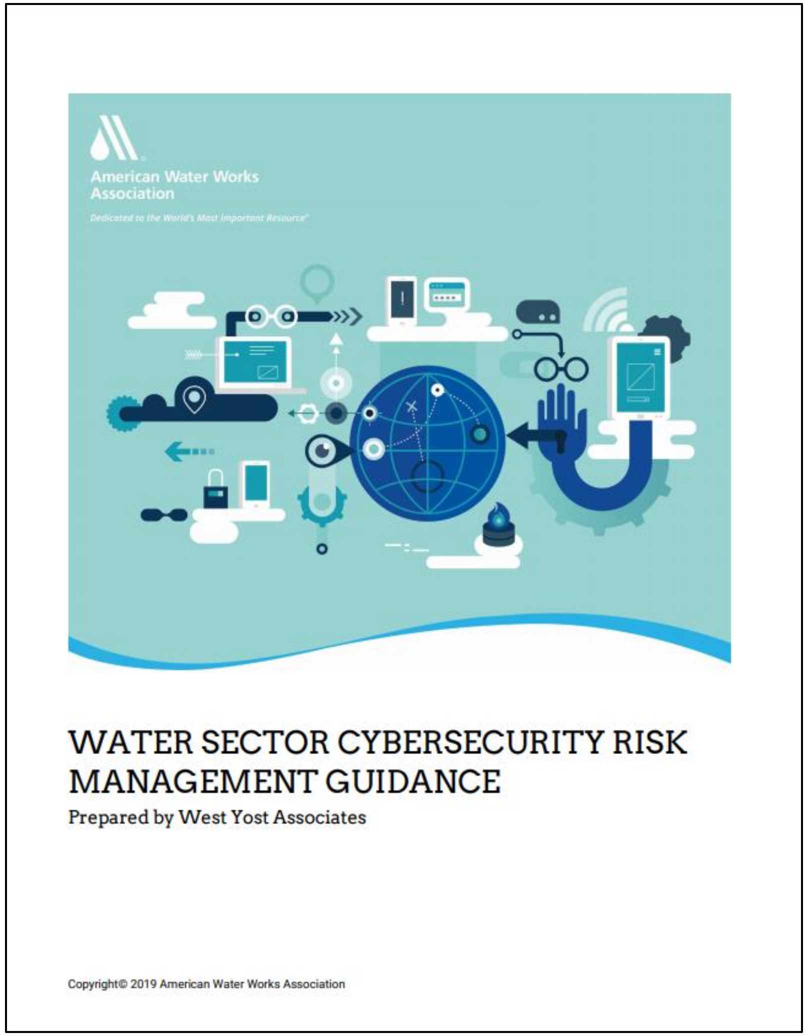
- **H.R. 2344**, Water System Threat Preparedness and Resilience Act

ANALYSIS

Key Steps

- ***Leadership commitment & culture***
- ***Build team to manage risk & resilience***
- ***Leverage resources for due diligence***
- **Assess vulnerabilities**
- **Make plan to mitigate vulnerabilities**
- **Develop & exercise response plan**

Implementing Best Practices = Due Diligence



American Water Works Association

Dedicated to the World's Most Important Resource®

WATER SECTOR CYBERSECURITY RISK MANAGEMENT GUIDANCE

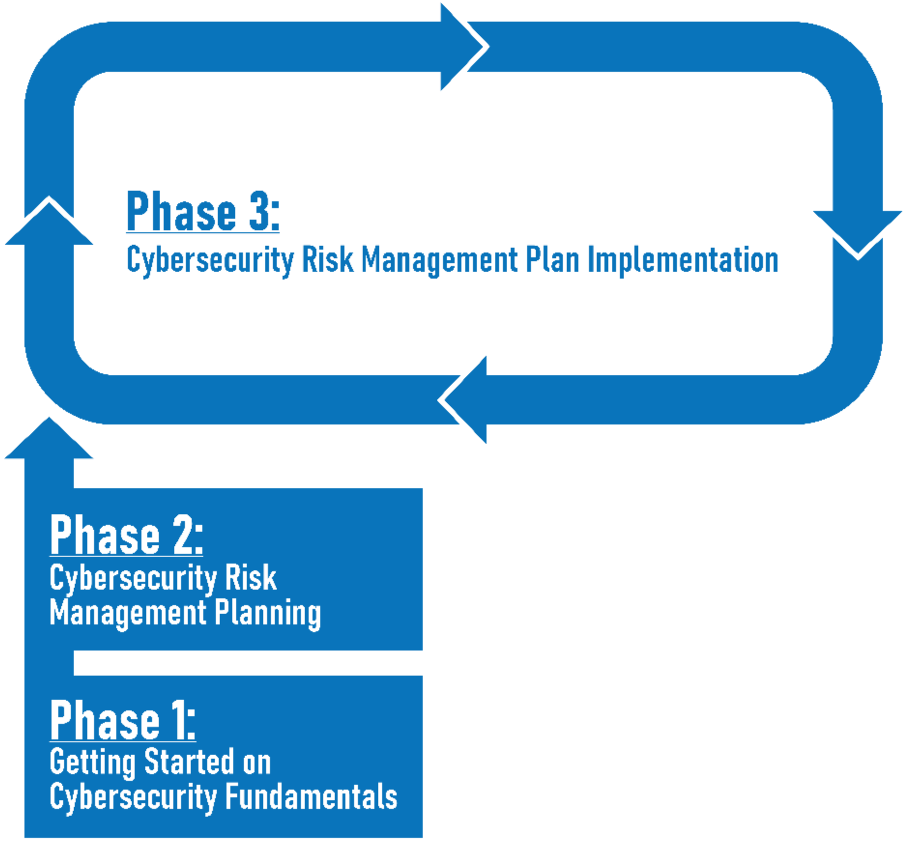
Prepared by West Yost Associates

- Provides a consistent and repeatable recommended course of action to recognize and mitigate cyber vulnerabilities

- **Recognized by NIST, USEPA, CISA**

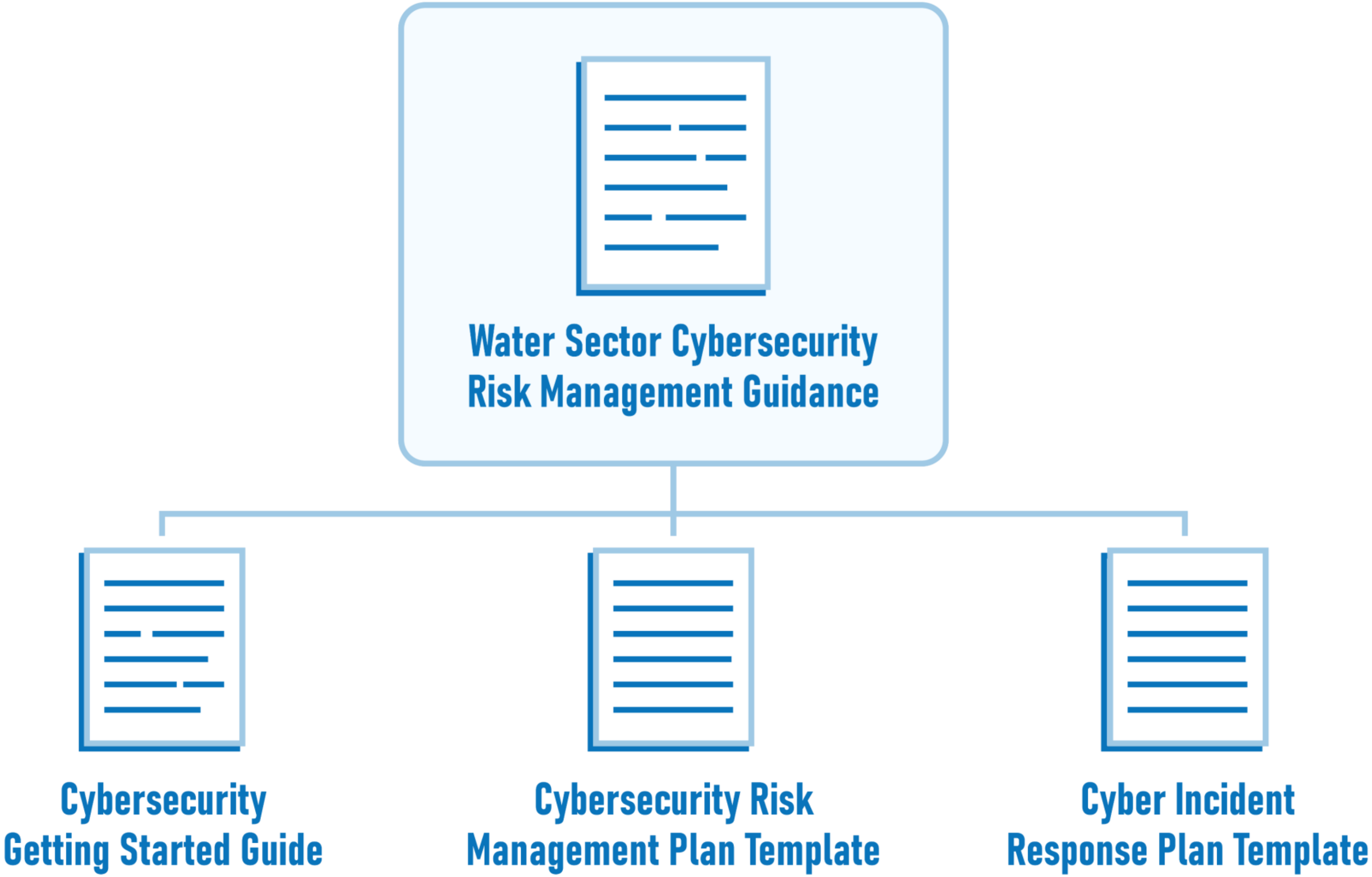
- **Prioritizes most relevant control based on 22 question about technology applications**

Priority Action on Technical Basics


Phase 3:
Cybersecurity Risk Management Plan Implementation
Phase 2:
Cybersecurity Risk Management Planning
Phase 1:
Getting Started on Cybersecurity Fundamentals

1. *Remove nonessential publicly facing devices from the internet and enroll in CISA's Vulnerability Scanning Service or similar program*
2. *Implement MFA, especially for remote access*
3. *Unique usernames and strong passwords*
4. *Assess vulnerability using available tools*
5. *Develop and exercise an Incident Response Plan*
6. *Change all default passwords when possible*
7. *Plan for and implement a network monitoring solution*
8. *Backup critical software and programs*

NEW AWWA CYBERSECURITY RESOURCE SUITE



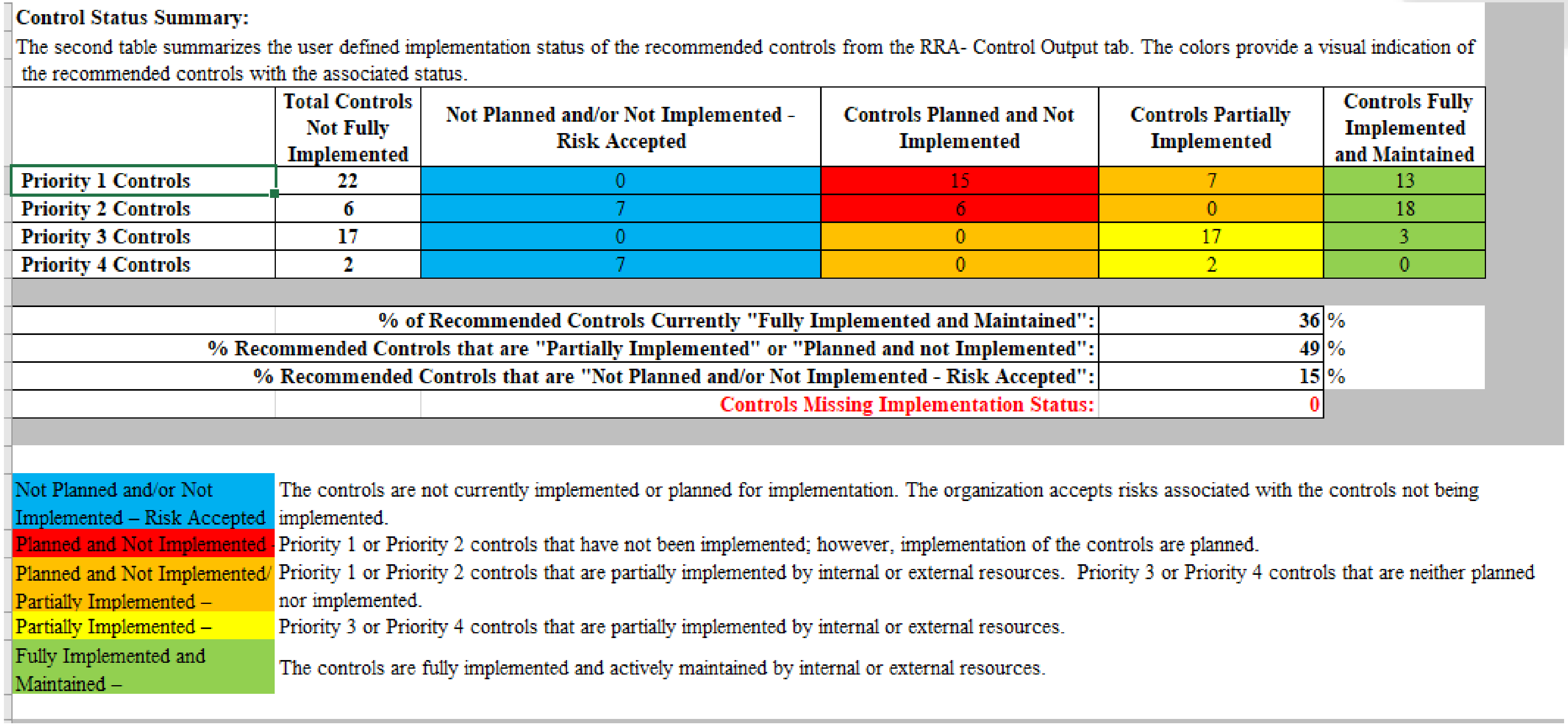
Water Sector Cybersecurity Risk Management Guidance

Cybersecurity Getting Started Guide

Cybersecurity Risk Management Plan Template

Cyber Incident Response Plan Template

CYBERSECURITY DUE DILIGENCE



Control Status Summary:

The second table summarizes the user defined implementation status of the recommended controls from the RRA- Control Output tab. The colors provide a visual indication of the recommended controls with the associated status.

	Total Controls Not Fully Implemented	Not Planned and/or Not Implemented - Risk Accepted	Controls Planned and Not Implemented	Controls Partially Implemented	Controls Fully Implemented and Maintained
Priority 1 Controls	22	0	15	7	13
Priority 2 Controls	6	7	6	0	18
Priority 3 Controls	17	0	0	17	3
Priority 4 Controls	2	7	0	2	0

% of Recommended Controls Currently "Fully Implemented and Maintained":	36	%
% Recommended Controls that are "Partially Implemented" or "Planned and not Implemented":	49	%
% Recommended Controls that are "Not Planned and/or Not Implemented - Risk Accepted":	15	%
Controls Missing Implementation Status:	0	

Not Planned and/or Not Implemented – Risk Accepted	The controls are not currently implemented or planned for implementation. The organization accepts risks associated with the controls not being implemented.
Planned and Not Implemented –	Priority 1 or Priority 2 controls that have not been implemented; however, implementation of the controls are planned.
Planned and Not Implemented/ Partially Implemented –	Priority 1 or Priority 2 controls that are partially implemented by internal or external resources. Priority 3 or Priority 4 controls that are neither planned nor implemented.
Partially Implemented –	Priority 3 or Priority 4 controls that are partially implemented by internal or external resources.
Fully Implemented and Maintained –	The controls are fully implemented and actively maintained by internal or external resources.

www.awwa.org/cybersecurity

?? QUESTIONS ??

Kevin M. Morley, PhD

Manager, Federal Relations
AWWA – Government Affairs
kmorley@awwa.org

www.awwa.org/cybersecurity
www.awwa.org/risk
www.cisa.gov/water
www.epa.gov/waterresilience/epa-cybersecurity-water-sector
www.waterisac.org