Managing the Legal Liabilities Associated with Cyber Attacks

October 2023 OTCO Compliance Workshop

presented by:
Matthew A. Dooley

DOOLEY GEMBALA
McLAUGHLIN PECORA
ATTORNEYS & COUNSELORS

www.dooleygembala.com

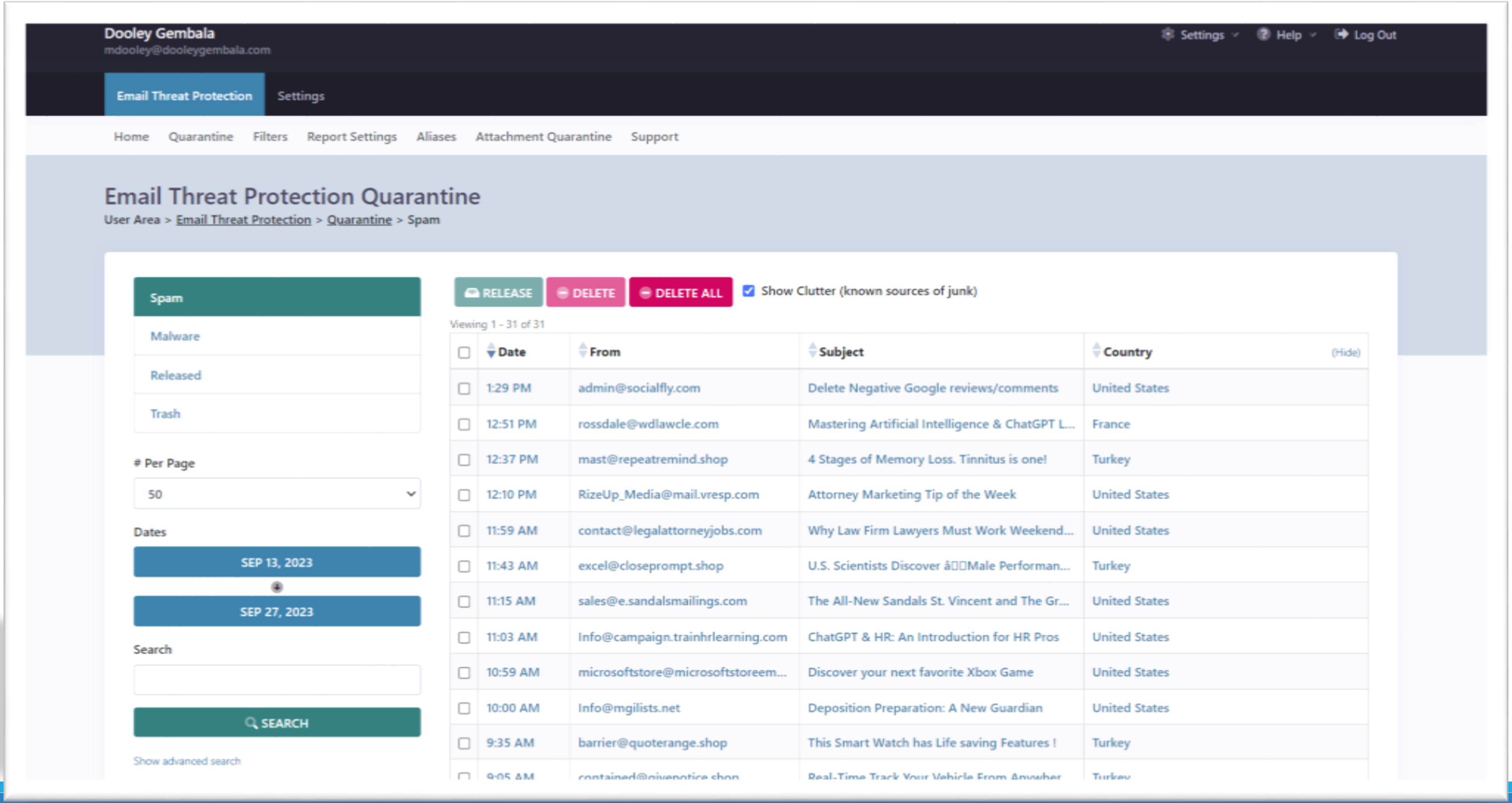
What are the Risks?

- Interruption of treatment, distribution or conveyance processes from opening and closing valves, overriding alarms, or disabling pumps.
- Theft of customer PII and credit card information
- Defacement of utility website or compromising email systems
- Inability to access and use SCADA for remote monitoring
- Fraudulent money transfers

What is Ransomware?

- 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.
- Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid.
- Attacks on government entities are increasing.
- The federal government provides regular updates and guidance at https://www.cisa.gov/stopransomware/resources.

Isolate Threats



Email Threat Protection Quarantine

User Area > Email Threat Protection > Quarantine > Spam

# Per Page: 50

Dates: SEP 13, 2023 – SEP 27, 2023

Search:

☑ Show Clutter (known sources of junk)

Viewing 1 - 31 of 31

□	Date	From	Subject	Country (Hide)
□	1:29 PM	admin@socialfly.com	Delete Negative Google reviews/comments	United States
□	12:51 PM	rossdale@wdlawcle.com	Mastering Artificial Intelligence & ChatGPT L...	France
□	12:37 PM	mast@repeatremind.shop	4 Stages of Memory Loss. Tinnitus is one!	Turkey
□	12:10 PM	RizeUp_Media@mail.vresp.com	Attorney Marketing Tip of the Week	United States
□	11:59 AM	contact@legalattorneyjobs.com	Why Law Firm Lawyers Must Work Weekend...	United States
□	11:43 AM	excel@closeprompt.shop	U.S. Scientists Discover â□□Male Performan...	Turkey
□	11:15 AM	sales@e.sandalsmailings.com	The All-New Sandals St. Vincent and The Gr...	United States
□	11:03 AM	Info@campaign.trainhrlearning.com	ChatGPT & HR: An Introduction for HR Pros	United States
□	10:59 AM	microsoftstore@microsoftstoreem...	Discover your next favorite Xbox Game	United States
□	10:00 AM	Info@mgilists.net	Deposition Preparation: A New Guardian	United States
□	9:35 AM	barrier@quoterange.shop	This Smart Watch has Life saving Features !	Turkey
□	9:05 AM	contained@givenotice.shop	Real-Time Track Your Vehicle From Anywher	Turkey

Additional Steps to Prepare

- Identify mission critical IT systems and key personnel responsible for operating and maintaining each system
- Designate a lead to enforce IT security protocols, including MFA, anti-virus, malware prevention
- Review and update the cybersecurity elements of your emergency response plan
- Limit employee access to systems if not necessary to perform job functions, especially remote access
- Provide training to identify potential threats and consider conducting drills
- Backup data regularly using cloud or offsite systems

Guard All Assessments

- FOIA and state law equivalents exclude confidential information from disclosure.
- This is particularly true for details related to critical infrastructure.
- Limit employee access as well to minimize chance for leaks.
- Do not discuss detailed threat assessments or vulnerability findings in public meetings.

Immediate Response Tactics

- Disconnect compromised computers from the network, but do not reboot
- Notify IT lead tasked with handling emergency response
- Assess damage level and effected stakeholders
- Provide notice to appropriate state and federal authorities, including DHS CISA
- Document as much as possible about the incident, including suspicious activity leading to hack
- Contact any pertinent insurance carrier
- Provide notice to impacted individuals regarding unauthorized access to PII
- Report the incident to Water Information sharing and Analysis Center

September 26, 2023 WaterISAC Report

- September is Insider Threat Awareness Month
- Average annual cost of insider threat has increased to $16.2 million
- Increased 40% in last four years
- Average number of days to contain and recover from insider incident is 86 days
- 88% of organizations spent less than 10% of their total IT security budget on insider threat management
- 75% of survey respondents reported threats caused by employee negligence or naivety

Recent Examples of Cyber Attacks to Water Authorities

Oldsmar, Florida
(February 8, 2021)
Attempt to change levels of sodium hydroxide by cyberattack – No findings attack occurred.

Discovery Bay, California
(January 2021)
Intentional removal of main operational and monitoring system for the Water Treatment Plant – Indictment of employee.

US-Canada Water Commission Investigating Cyberattack
(September 11, 2023)

Ransomware attacks

Still under investigation

Discovery Bay, California (January 2021):

- A federal grand jury has indicted Rambler Gallo, charging him with intentionally causing damage to a protected computer after he accessed the computer network for the Discovery Bay Water Treatment Facility and intentionally uninstalled the main operational and monitoring system for the water treatment plant and then turned off the servers running those systems causing a threat to public health and safety.
- According to the indictment, filed June 27, 2023, prior to the attack on the Discovery Bay Water Treatment facility, Gallo was a full-time employee of a private Massachusetts-based company identified in the indictment as Company A.
- Company A contracted with Discovery Bay to operate the town’s wastewater treatment facility; the facility provides treatment for the water and wastewater systems for the town’s 15,000 residents.

DISCOVERY BAY, CALIFORNIA (JANUARY 2021):

- While Gallo was employed with Company A, he installed software on his own personal computer and on Company A's private internal network that allowed him to gain remote access to Discovery Bay's Water Treatment facility computer network.
- After Gallo resigned from Company A, he accessed the facility's computer system remotely and transmitted a command to uninstall software that was the main hub of the facility's computer network and that protected the entire water treatment system, including water pressure, filtration, and chemical levels.
- The indictment charges Gallo with one count of transmitting a program, information, code, and command to cause damage to a protected computer, in violation of 18 U.S.C. §§ 1030(a)(5)(A) and (c)(4)(B)(i).
- If convicted, Gallo faces a maximum statutory penalty of 10 years in prison and a fine of $250,000

Oldsmar, Florida (February 8, 2021)

- An operator noticed his cursor moving around on the screen followed by adjustments to the sodium hydroxide levels.
- He quickly spotted the intrusion and returned the sodium hydroxide to normal levels.
- There have been recent reports that this hacking never occurred.
- Former Oldsmar City Manager, Al Braithwaite, said this year it wasn’t a cyber attack.
- Some suggest that the sodium hydroxide increase was due to an employee’s mistake.

US-Canada Water Commission Investigating Cyberattack (September 11, 2023):

- The organization tasked with managing the lake and river systems along the border between the U.S. and Canada for the last hundred years announced it experienced a cyberattack following reports that ransomware hackers claimed to have stolen reams of data.
- The International Joint Commission (IJC) approves projects that affect the water levels and flows across the border, investigates transboundary issues and offers solutions.
- On September 11, 2023, the NoEscape ransomware gang claimed it attacked the organization and stole 80 GB of contracts, geological files, conflict of interest forms and more.
- The gang gave the IJC 10 days to respond to their demand for a ransom.

HISTORY OF CONGRESS'S CYBERSECURITY FRAMEWORK FOR WATER SYSTEMS

Safe Drinking Water Act (“SDWA”) Amendments

2002

>3,300 Customers

- CWS to submit threat Assessment to EPA
- Prepare/revise Emergency Response Plan (ERP)

<3,300 Customers

- EPA to provide guidance on how to conduct ERP

42 U.S.C. § 300i-2(a)(1)(2002)

America's Water Infrastructure Act

2018

- Expansion of risk types to be evaluated
- Evaluate resilience of systems
- Review and update ERPs every 5 years
- Increase of cybersecurity asset scope
- EPA limited to certification of ERPs

42 U.S.C. § 300i-2(a)(1)(2018)

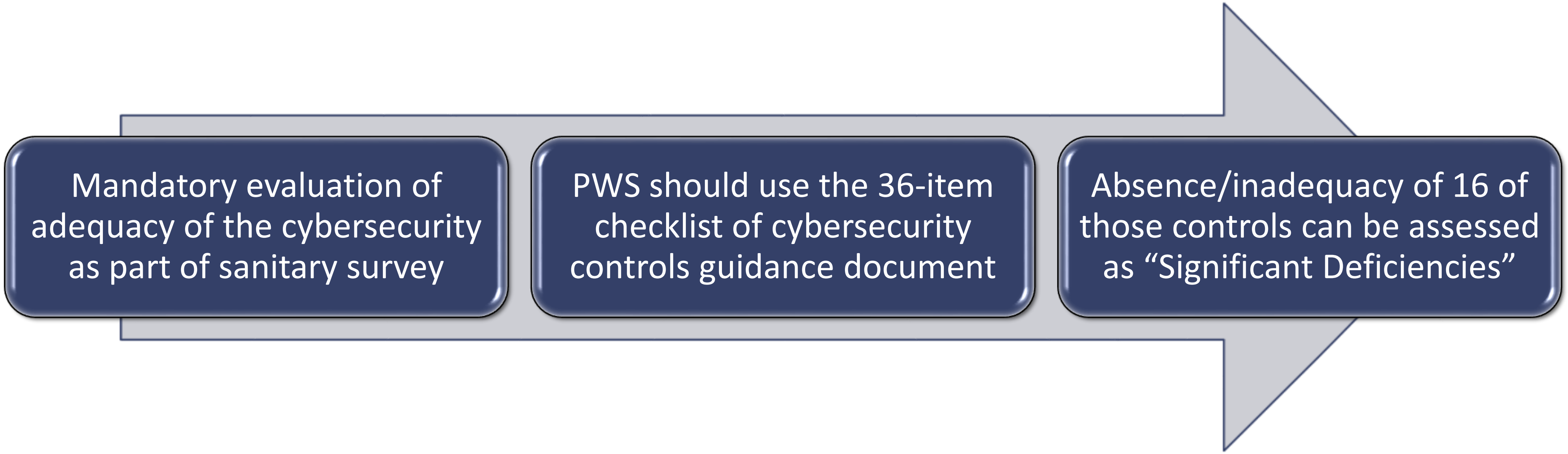
EPA Guidance

2023

- State must conduct periodic audits “Sanitary surveys”.

March 2, 2023 EPA Memorandum

Applies to all public water systems of all sizes



Mandatory evaluation of adequacy of the cybersecurity as part of sanitary survey

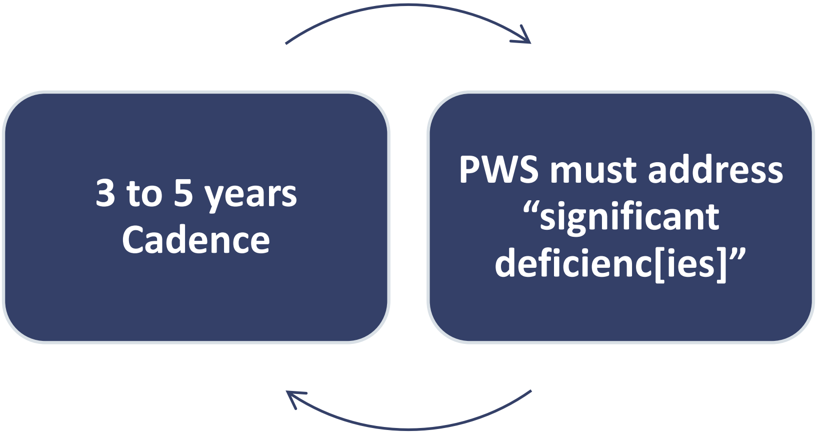
PWS should use the 36-item checklist of cybersecurity controls guidance document

Absence/inadequacy of 16 of those controls can be assessed as “Significant Deficiencies”

What is the Sanitary Survey Program?

“[A]n onsite review of the water source, facilities, equipment, operation and maintenance of a [PWS] for the purpose of evaluating the adequacy of such source, facilities, equipment, operation and maintenance for producing and distributing safe drinking water.”

40 C.F.R. §§ 141.2, 142.16(b)(3).



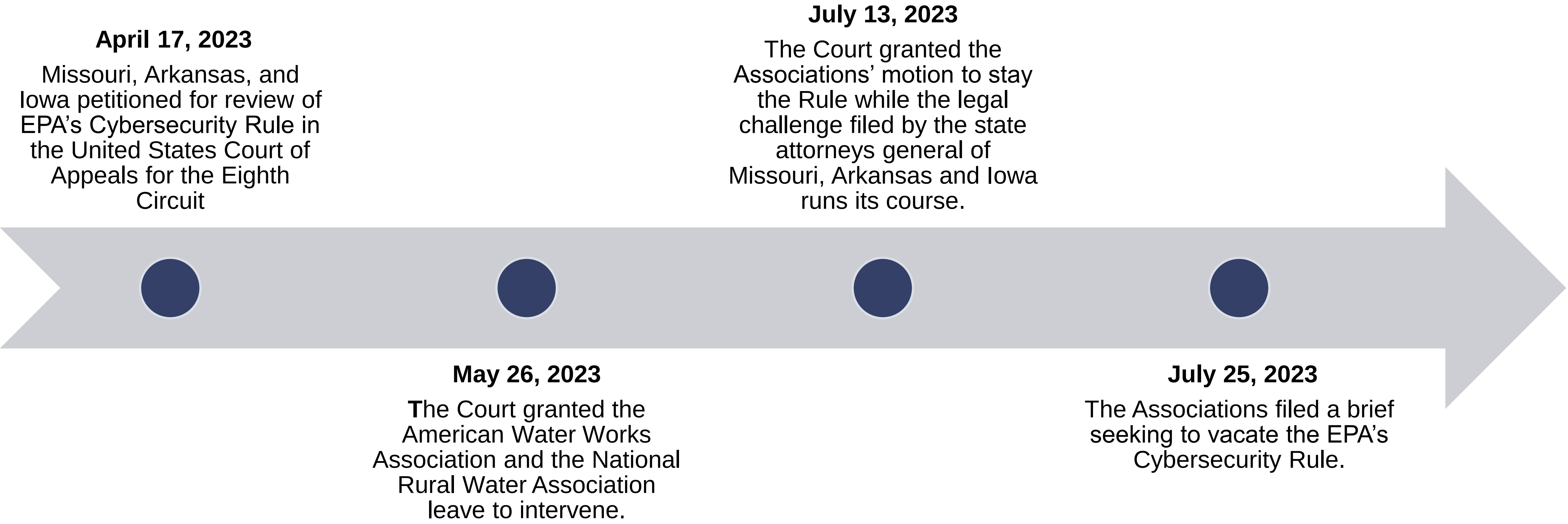
3 to 5 years Cadence

PWS must address “significant deficienc[ies]”

Risk of Finding Significant Deficiency

1. Enforcement Actions
2. Decrease in Customer Confidence
3. Lower Credit Ratings

RECENT COURT CHALLENGES TO THE EPA CYBERSECURITY RULE



April 17, 2023

Missouri, Arkansas, and Iowa petitioned for review of EPA's Cybersecurity Rule in the United States Court of Appeals for the Eighth Circuit

May 26, 2023

The Court granted the American Water Works Association and the National Rural Water Association leave to intervene.

July 13, 2023

The Court granted the Associations' motion to stay the Rule while the legal challenge filed by the state attorneys general of Missouri, Arkansas and Iowa runs its course.

July 25, 2023

The Associations filed a brief seeking to vacate the EPA's Cybersecurity Rule.

Legal Argument Against the EPA Cybersecurity Rule

Legislative not “interpretive” – exceeds EPA’s authority under the SDWA.

Lack of expertise from state regulators – could lead to inaccurate “significant deficiency” findings.

Hardship for PWS to obtain funding to meet new standards.

Confidentiality concerns with EPA reporting of specific cybersecurity vulnerabilities.

Overreach for CWS serving less than 3,300 customers – Requirements not intended by Congress.

Litigation Avoidance

- Data breach litigation is a cottage industry for lawyers.
- Damage to an individual’s credit worthiness can be devastating.
- A negligent standard normally applies – what would an ordinarily prudent person do to manage foreseeable risks?
- The risks of cyberattacks is more foreseeable now than ever.
- Setting aside the EPA’s rule, utilities must take steps to mitigate against threats to avoid adverse litigation outcomes.
- Purchase cyber insurance and follow all policy requirements, even if annoying on a day-to-day basis.
- Consider whether coverage includes ransom payments, indemnification against claims, and business interruption losses.

Free Vulnerability Scanning Services

Offered by Cybersecurity and Infrastructure Security Agency (CISA)

Water systems can get weekly automated scans that will provide a report on known vulnerabilities found on internet-accessible assets, week-to-week comparisons, and mitigations.

How to get started?

1

Send an Email to:
vulnerability@cisa.dhs.gov

Subject: “Requesting Vulnerability Scanning Services.”

Add: name of your utility, point of contact with an email address + 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

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

REPORT CARD
CISA
August 30, 2022 — November 26, 2022
November 20, 2022 — November 26, 2022
0
1
0%
8,976
8,976
35
71
25
122
DRAFT
2027 DAYS
2473 DAYS

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 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

QUESTIONS?

Feel free to reach out via phone or email anytime with additional questions:

(440) 930-4001

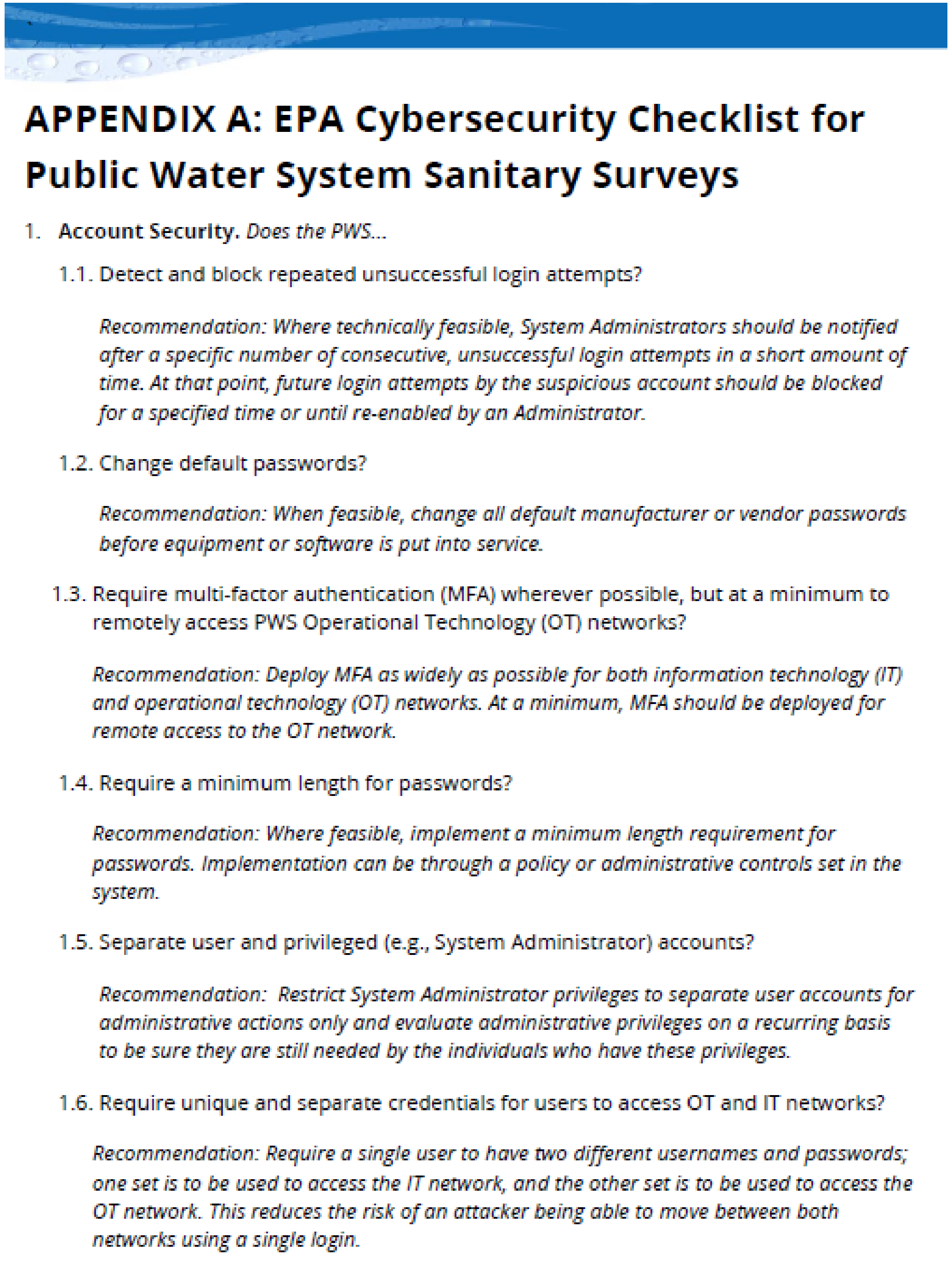
mdooley@dooleygembala.com

DOOLEY GEMBALA McLAUGHLIN PECORA
ATTORNEYS & COUNSELORS

www.dooleygembala.com

Appendix

EPA’s Cybersecurity Checklist for Sanitary Survey



APPENDIX A: EPA Cybersecurity Checklist for Public Water System Sanitary Surveys

1. **Account Security.** *Does the PWS…*

   1.1. Detect and block repeated unsuccessful login attempts?

   Recommendation: Where technically feasible, System Administrators should be notified after a specific number of consecutive, unsuccessful login attempts in a short amount of time. At that point, future login attempts by the suspicious account should be blocked for a specified time or until re-enabled by an Administrator.

   1.2. Change default passwords?

   Recommendation: When feasible, change all default manufacturer or vendor passwords before equipment or software is put into service.

   1.3. Require multi-factor authentication (MFA) wherever possible, but at a minimum to remotely access PWS Operational Technology (OT) networks?

   Recommendation: Deploy MFA as widely as possible for both information technology (IT) and operational technology (OT) networks. At a minimum, MFA should be deployed for remote access to the OT network.

   1.4. Require a minimum length for passwords?

   Recommendation: Where feasible, implement a minimum length requirement for passwords. Implementation can be through a policy or administrative controls set in the system.

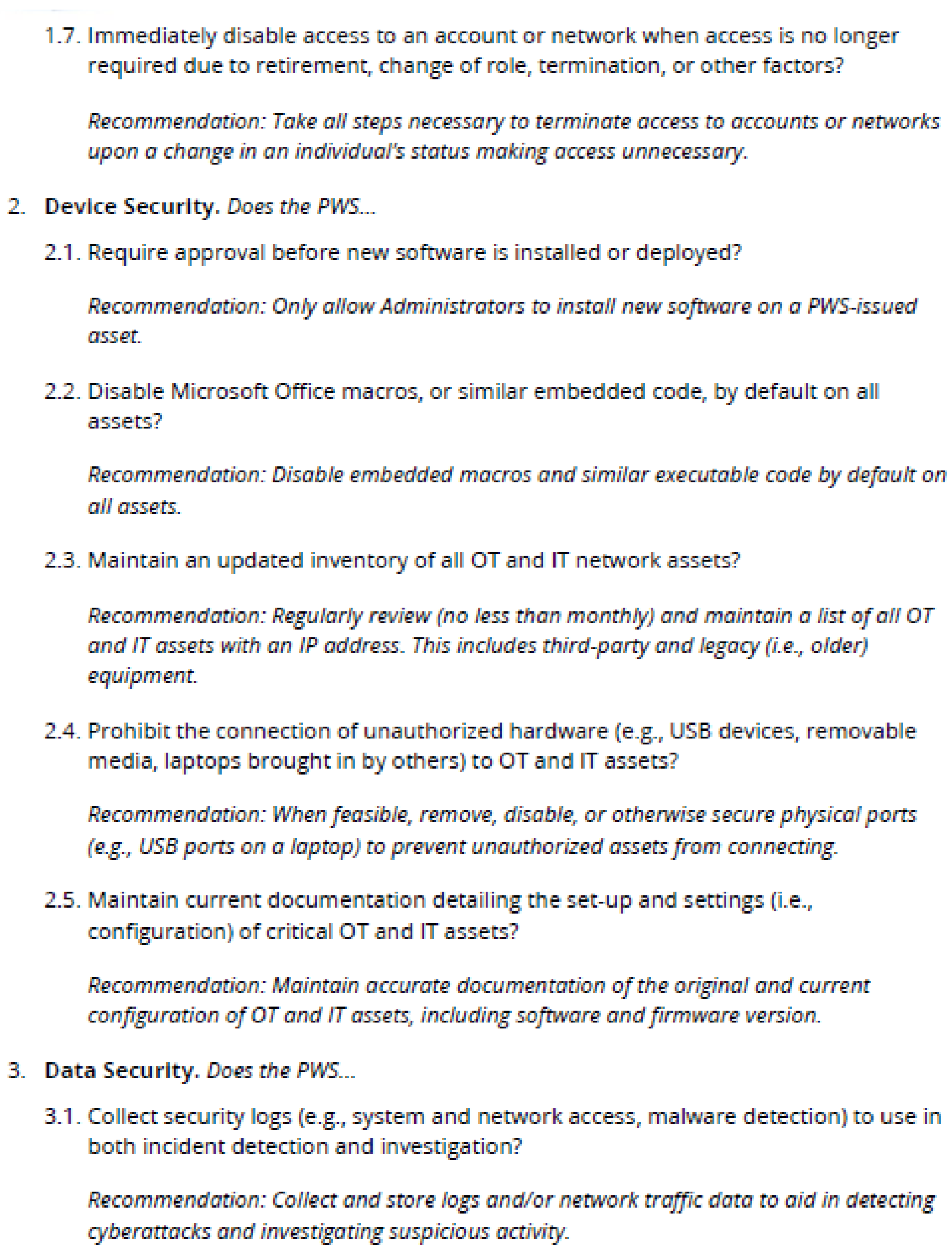
   1.5. Separate user and privileged (e.g., System Administrator) accounts?

   Recommendation: Restrict System Administrator privileges to separate user accounts for administrative actions only and evaluate administrative privileges on a recurring basis to be sure they are still needed by the individuals who have these privileges.

   1.6. Require unique and separate credentials for users to access OT and IT networks?

   Recommendation: Require a single user to have two different usernames and passwords; one set is to be used to access the IT network, and the other set is to be used to access the OT network. This reduces the risk of an attacker being able to move between both networks using a single login.

EPA's Cybersecurity Checklist for Sanitary Survey



1.7. Immediately disable access to an account or network when access is no longer required due to retirement, change of role, termination, or other factors?

Recommendation: Take all steps necessary to terminate access to accounts or networks upon a change in an individual's status making access unnecessary.

2. **Device Security.** *Does the PWS...*

2.1. Require approval before new software is installed or deployed?

Recommendation: Only allow Administrators to install new software on a PWS-issued asset.

2.2. Disable Microsoft Office macros, or similar embedded code, by default on all assets?

Recommendation: Disable embedded macros and similar executable code by default on all assets.

2.3. Maintain an updated inventory of all OT and IT network assets?

Recommendation: Regularly review (no less than monthly) and maintain a list of all OT and IT assets with an IP address. This includes third-party and legacy (i.e., older) equipment.

2.4. Prohibit the connection of unauthorized hardware (e.g., USB devices, removable media, laptops brought in by others) to OT and IT assets?

Recommendation: When feasible, remove, disable, or otherwise secure physical ports (e.g., USB ports on a laptop) to prevent unauthorized assets from connecting.

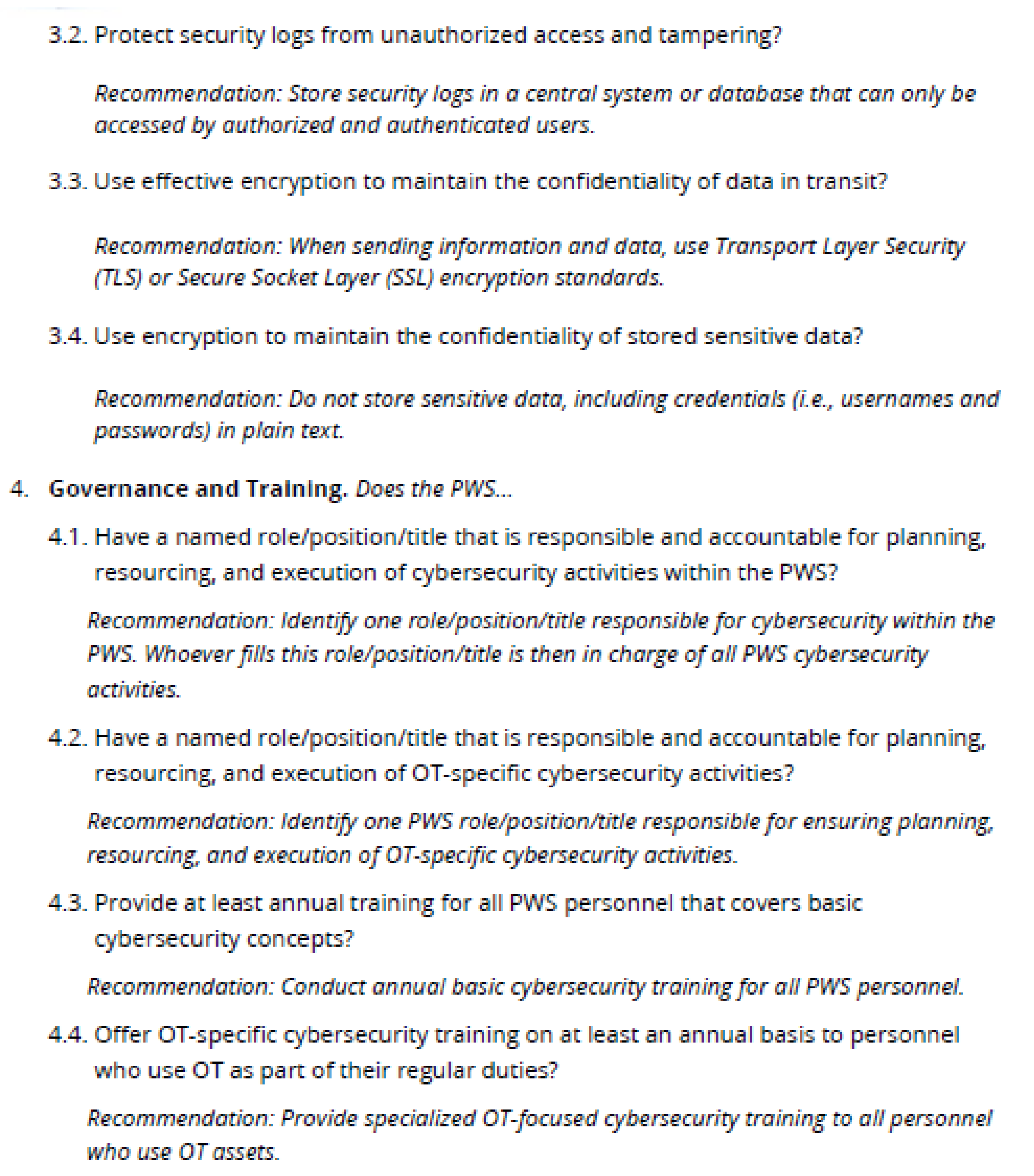
2.5. Maintain current documentation detailing the set-up and settings (i.e., configuration) of critical OT and IT assets?

Recommendation: Maintain accurate documentation of the original and current configuration of OT and IT assets, including software and firmware version.

3. **Data Security.** *Does the PWS...*

3.1. Collect security logs (e.g., system and network access, malware detection) to use in both incident detection and investigation?

Recommendation: Collect and store logs and/or network traffic data to aid in detecting cyberattacks and investigating suspicious activity.



3.2. Protect security logs from unauthorized access and tampering?

Recommendation: Store security logs in a central system or database that can only be accessed by authorized and authenticated users.

3.3. Use effective encryption to maintain the confidentiality of data in transit?

Recommendation: When sending information and data, use Transport Layer Security (TLS) or Secure Socket Layer (SSL) encryption standards.

3.4. Use encryption to maintain the confidentiality of stored sensitive data?

Recommendation: Do not store sensitive data, including credentials (i.e., usernames and passwords) in plain text.

4. **Governance and Training.** *Does the PWS...*

4.1. Have a named role/position/title that is responsible and accountable for planning, resourcing, and execution of cybersecurity activities within the PWS?

Recommendation: Identify one role/position/title responsible for cybersecurity within the PWS. Whoever fills this role/position/title is then in charge of all PWS cybersecurity activities.

4.2. Have a named role/position/title that is responsible and accountable for planning, resourcing, and execution of OT-specific cybersecurity activities?

Recommendation: Identify one PWS role/position/title responsible for ensuring planning, resourcing, and execution of OT-specific cybersecurity activities.

4.3. Provide at least annual training for all PWS personnel that covers basic cybersecurity concepts?

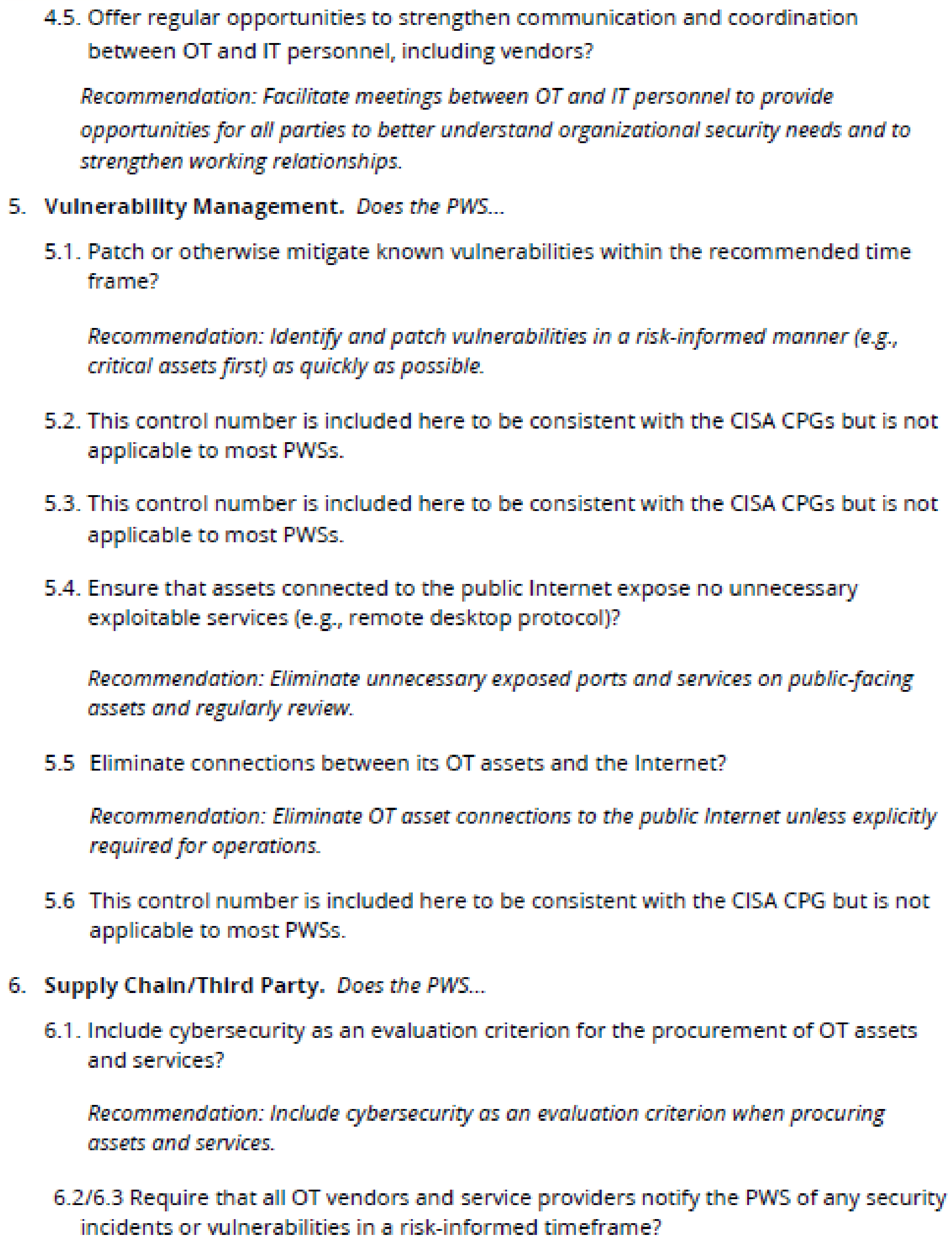
Recommendation: Conduct annual basic cybersecurity training for all PWS personnel.

4.4. Offer OT-specific cybersecurity training on at least an annual basis to personnel who use OT as part of their regular duties?

Recommendation: Provide specialized OT-focused cybersecurity training to all personnel who use OT assets.

EPA's Cybersecurity Checklist for Sanitary Survey

EPA’s Cybersecurity Checklist for Sanitary Survey



4.5. Offer regular opportunities to strengthen communication and coordination between OT and IT personnel, including vendors?

Recommendation: Facilitate meetings between OT and IT personnel to provide opportunities for all parties to better understand organizational security needs and to strengthen working relationships.

5. **Vulnerability Management.** *Does the PWS…*

5.1. Patch or otherwise mitigate known vulnerabilities within the recommended time frame?

Recommendation: Identify and patch vulnerabilities in a risk-informed manner (e.g., critical assets first) as quickly as possible.

5.2. This control number is included here to be consistent with the CISA CPGs but is not applicable to most PWSs.

5.3. This control number is included here to be consistent with the CISA CPGs but is not applicable to most PWSs.

5.4. Ensure that assets connected to the public Internet expose no unnecessary exploitable services (e.g., remote desktop protocol)?

Recommendation: Eliminate unnecessary exposed ports and services on public-facing assets and regularly review.

5.5 Eliminate connections between its OT assets and the Internet?

Recommendation: Eliminate OT asset connections to the public Internet unless explicitly required for operations.

5.6 This control number is included here to be consistent with the CISA CPG but is not applicable to most PWSs.

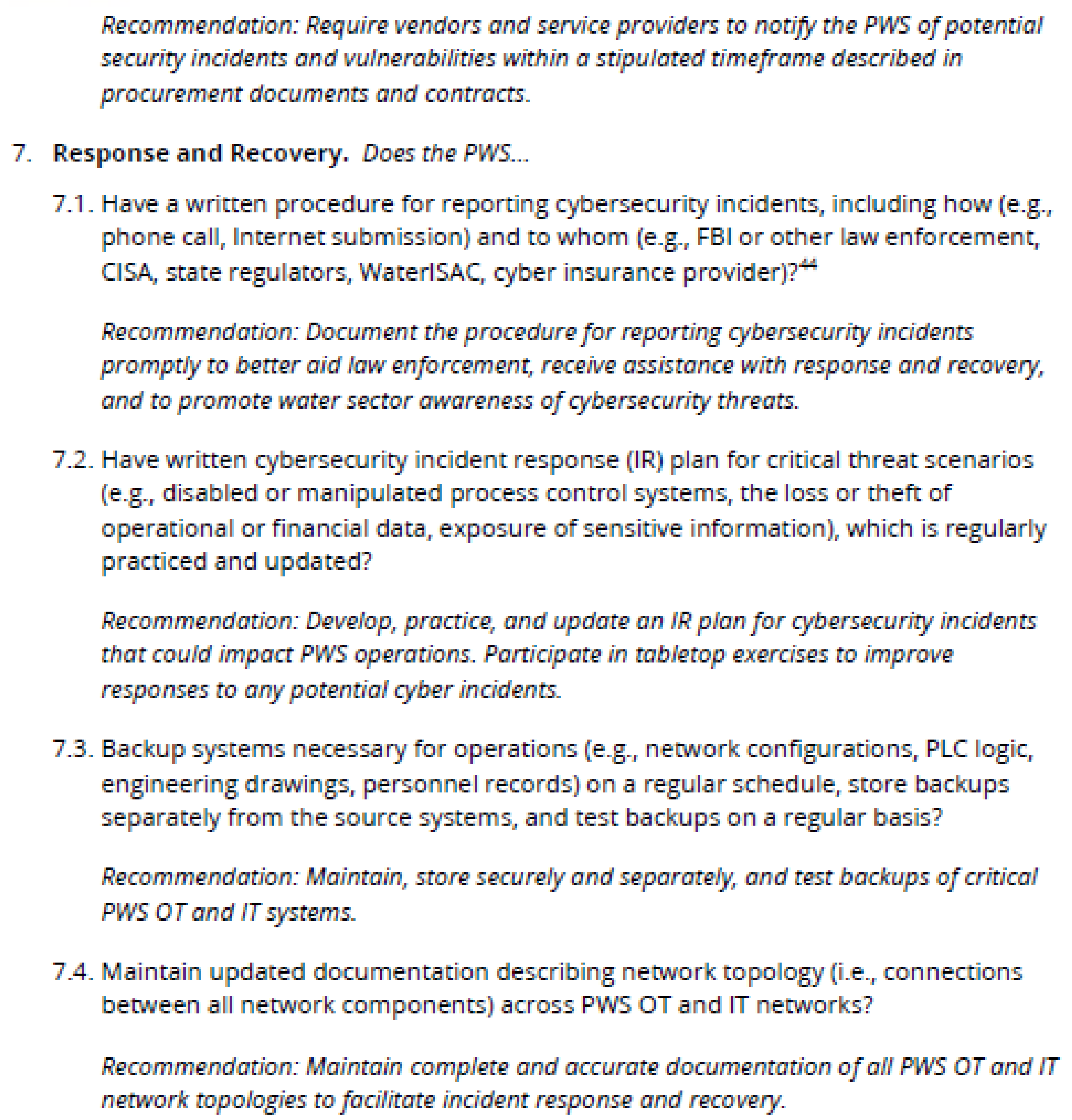
6. **Supply Chain/Third Party.** *Does the PWS…*

6.1. Include cybersecurity as an evaluation criterion for the procurement of OT assets and services?

Recommendation: Include cybersecurity as an evaluation criterion when procuring assets and services.

6.2/6.3 Require that all OT vendors and service providers notify the PWS of any security incidents or vulnerabilities in a risk-informed timeframe?

EPA's Cybersecurity Checklist for Sanitary Survey



Recommendation: Require vendors and service providers to notify the PWS of potential security incidents and vulnerabilities within a stipulated timeframe described in procurement documents and contracts.

7. **Response and Recovery.** *Does the PWS...*

7.1. 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)?[44]

Recommendation: Document the procedure for reporting cybersecurity incidents promptly to better aid law enforcement, receive assistance with response and recovery, and to promote water sector awareness of cybersecurity threats.

7.2. Have written cybersecurity incident response (IR) 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 practiced and updated?

Recommendation: Develop, practice, and update an IR plan for cybersecurity incidents that could impact PWS operations. Participate in tabletop exercises to improve responses to any potential cyber incidents.

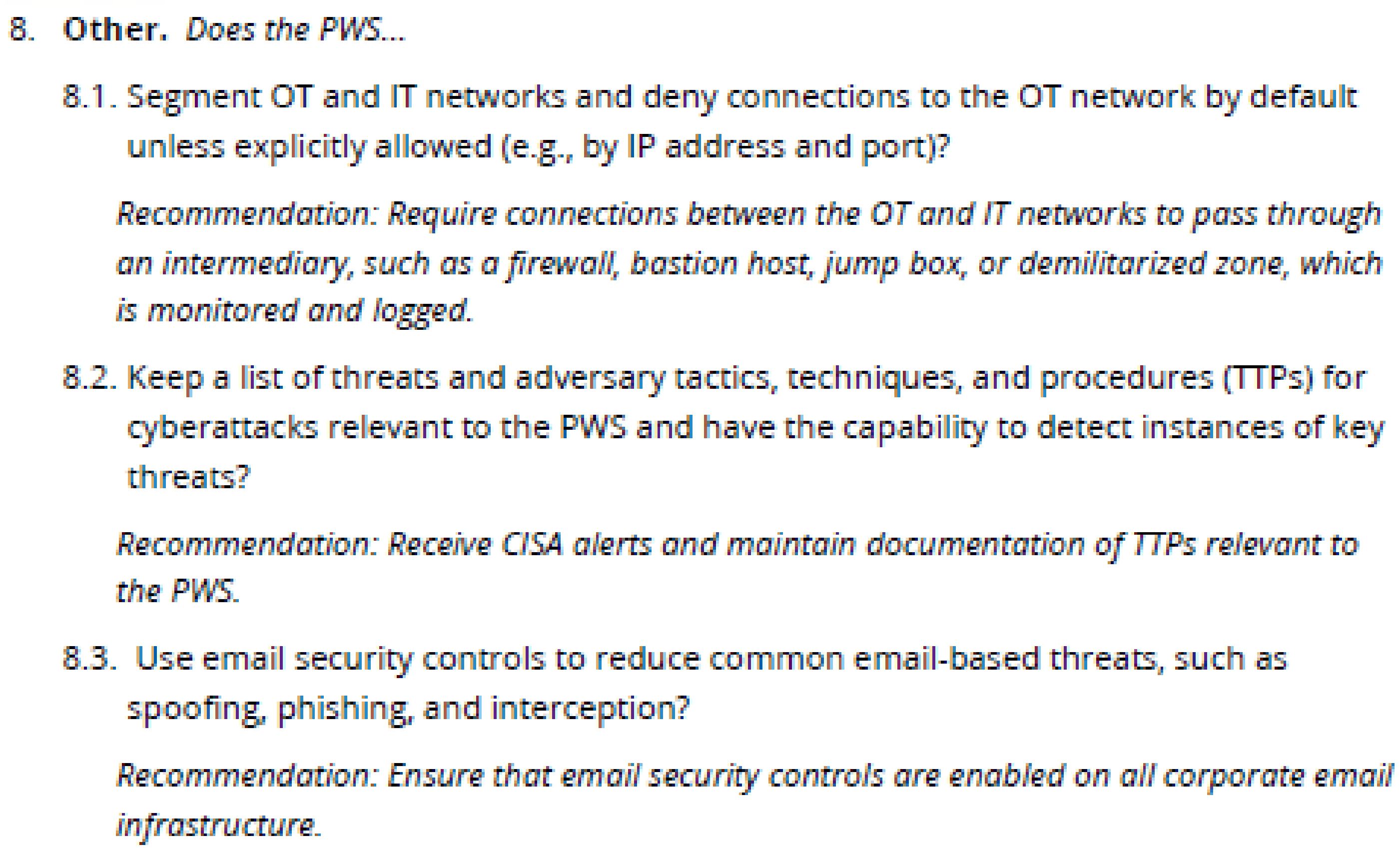
7.3. Backup systems necessary for operations (e.g., network configurations, PLC logic, engineering drawings, personnel records) on a regular schedule, store backups separately from the source systems, and test backups on a regular basis?

Recommendation: Maintain, store securely and separately, and test backups of critical PWS OT and IT systems.

7.4. Maintain updated documentation describing network topology (i.e., connections between all network components) across PWS OT and IT networks?

Recommendation: Maintain complete and accurate documentation of all PWS OT and IT network topologies to facilitate incident response and recovery.

EPA’s Cybersecurity Checklist for Sanitary Survey



8. **Other.** *Does the PWS…*

   8.1. Segment OT and IT networks and deny connections to the OT network by default unless explicitly allowed (e.g., by IP address and port)?

   Recommendation: Require connections between the OT and IT networks to pass through an intermediary, such as a firewall, bastion host, jump box, or demilitarized zone, which is monitored and logged.

   8.2. Keep a list of threats and adversary tactics, techniques, and procedures (TTPs) for cyberattacks relevant to the PWS and have the capability to detect instances of key threats?

   Recommendation: Receive CISA alerts and maintain documentation of TTPs relevant to the PWS.

   8.3. Use email security controls to reduce common email-based threats, such as spoofing, phishing, and interception?

   Recommendation: Ensure that email security controls are enabled on all corporate email infrastructure.