Evaluating Cybersecurity During Public Water System Sanitary Surveys

EPA Office of Water (4608T)
EPA 817-B-23-001
February 2023

Disclaimer

The Water Infrastructure and Cyber Resilience Division of the Office of Ground Water and Drinking Water reviewed and approved this document for publication. This document does not impose legally binding requirements on any party. Neither the United States Government nor any of its employees, contractors or their employees make any warranty, expressed or implied, or assume any legal liability or responsibility for any third party's use of any information, product, or process discussed in this document, or represent that its use by such party would not infringe on privately owned rights. Mention of trade names or commercial products does not constitute endorsement or recommendation for use.

Public Comment

EPA invites public comment on Sections 4 - 8 and all Appendices of this guidance document. EPA plans to revise and update this document as needed based on public comment and new information. Comments regarding this document should be addressed to wicrd-outreach@epa.gov.

Table of Contents

1.0 Background 1

1.1. What is the purpose of this guidance? 1

1.2. Who should use this guidance? 1

2.0 What is the requirement to evaluate cybersecurity during PWS sanitary surveys? 2

3.0 What approaches can states follow to include cybersecurity in PWS sanitary surveys? .. 4

3.1. Option 1: PWS self-assessment or third-party assessment of cybersecurity practices 4

3.2. Option 2: State evaluation of cybersecurity practices during the sanitary survey 6

3.3. Option 3: Alternative state program for water system cybersecurity 6

3.4. Changes to state recordkeeping and reporting 7

4.0 Technical support for cybersecurity in PWS sanitary surveys 7

4.1. Training 7

4.2. Technical assistance 8

4.3. Additional resources 8

5.0 EPA Cybersecurity Checklist for Public Water System Sanitary Surveys 10

5.1. What is the purpose of this checklist? 10

5.2. The Checklist 11

6.0 Recommended alternatives to the EPA Checklist 11

7.0 Potential significant deficiencies 11

8.0 How should states protect sensitive information on PWS cybersecurity? 14

Appendices

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

Appendix B: Checklist Fact Sheets

Appendix C: Glossary of Terms

1.0 Background

1.1. What is the purpose of this guidance?

This guidance supports implementation of the U.S. Environmental Protection Agency (EPA) memorandum (memo), *Addressing PWS Cybersecurity in Sanitary Surveys or an Alternate Process*.[1] The steps described in the memo further EPA's mission to work with states[2] to protect clean and safe drinking water. The memo clarifies that states must evaluate the cybersecurity of operational technology[3] used by a public water system (PWS) when conducting a PWS sanitary survey or through other state programs.

The memo and this guidance explain various approaches to include cybersecurity in PWS sanitary surveys or other state programs. The goal of sanitary surveys is to ensure that states effectively identify significant deficiencies and that PWSs then correct those significant deficiencies —including cybersecurity-related significant deficiencies— that could impact safe drinking water. EPA is offering significant technical assistance and support to states in this effort, as well as to PWSs to help close cybersecurity gaps.

Today, PWSs are frequent targets of malicious cyber activity,[4] which has the same or even greater potential to compromise the treatment and distribution of safe drinking water as a physical attack. Clarifying that cybersecurity must be evaluated during sanitary surveys or other state programs when reviewing operational technology that is part of a PWS's equipment or operation will help reduce the likelihood of a successful cyberattack on a PWS and improve recovery if a cyber incident occurs.

1.2. Who should use this guidance?

This guidance excerpts information from the memo and offers optional supplementary material to assist states and PWSs with addressing the cybersecurity of operational technology in PWS sanitary surveys. For general information about PWS sanitary surveys, including underlying regulations, survey components and frequency, and reference materials, see https://www.epa.gov/dwreginfo/sanitary-surveys.

---

[1] https://www.epa.gov/waterriskassessment/epa-cybersecurity-best-practices-water-sector

[2] "State" or "states" globally in this document includes tribes, territories, and EPA Regions where they have primary enforcement authority for public water systems.

[3] The term "operational technology" means hardware and software that detects or causes a change through the direct monitoring or control of physical devices, processes, and events in the enterprise. Internet of Things Cybersecurity Improvement Act of 2020, 15 U.S.C. § 271(3)(6) (Public Law 116-207).

[4] Alert (AA21-287A), Ongoing Cyber Threats to U.S. Water and Wastewater Systems, https://www.cisa.gov/uscert/ncas/alerts/aa21-287a

EPA intends for this guidance to aid both states and PWSs. Specifically, state personnel involved in planning, conducting, or reviewing PWS sanitary surveys may use this guidance to learn the following:

- Approaches for evaluating cybersecurity at PWSs to meet sanitary survey requirements, including resources that can assist states with cybersecurity evaluation,
- How to identify gaps in PWS cybersecurity, including possible significant deficiencies, and
- Actions that PWSs can take to address gaps in cybersecurity, including significant deficiencies if identified by the state.

PWSs may use this guidance to learn the following:

- How to assess current PWS cybersecurity practices and controls to identify gaps,
- Actions to develop a PWS cybersecurity risk mitigation plan for cybersecurity gaps, including significant deficiencies if identified by the state, and
- Resources that can assist with closing cybersecurity gaps.

Note: the memo and this supporting guidance focus on the assessment and improvement of cybersecurity of operational technology at PWSs through sanitary surveys or alternative state programs. It does not encompass all components necessary for a comprehensive critical infrastructure cybersecurity program, such as potential state roles in cyber incident reporting and response.

2.0 What is the requirement to evaluate cybersecurity during PWS sanitary surveys?

The definition of a sanitary survey is "an 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."[5] Pursuant to relevant regulatory requirements, states are required to conduct periodic sanitary surveys of PWSs.[6] EPA interprets the regulatory requirements relating to the conduct of sanitary surveys to require that when a PWS uses operational technology, such as an industrial control system (ICS), as part of the equipment or operation of any required component[7] of a sanitary survey, then the sanitary survey of

[5] 40 CFR § 141.2

[6] 40 CFR §§ 141.2, 142.16(b)(3), 142.16(o)(2).

[7] 40 CFR § 142.16(b)(3) and (o)(2) [required components are listed in the Addendum]

that PWS must include an evaluation of the adequacy of the cybersecurity of that operational technology for producing and distributing safe drinking water.

An "industrial control system" is an information system used to control industrial processes such as manufacturing, product handling, production, and distribution. ICSs include supervisory control and data acquisition systems, used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.[8]

Accordingly, during a sanitary survey of a PWS, states must do the following to comply with the requirement to conduct a sanitary survey:

(1) If the PWS uses an ICS or other operational technology as part of the equipment or operation of any required component of the sanitary survey, then the state must evaluate the adequacy of the cybersecurity of that operational technology for producing and distributing safe drinking water.

(2) If the state determines that a cybersecurity deficiency identified during a sanitary survey is significant, then the state must use its authority to require the PWS to address the significant deficiency.[9]

EPA has defined "significant deficiencies" as including, but not limited to, "defects in design, operation, or maintenance, or a failure or malfunction of the sources, treatment, storage, or distribution system that the state determines to be causing, or have potential for causing, the introduction of contamination into the water delivered to consumers."[10] For cybersecurity, significant deficiencies should include the absence of a practice or control, or the presence of a vulnerability, that has a high risk of being exploited, either directly or indirectly, to compromise an operational technology used in the treatment or distribution of drinking water.

As described in Section 3, states can fulfill the responsibility to evaluate cybersecurity through different approaches conducted under their sanitary survey programs. Alternatively, states may meet this requirement by using an existing or establishing a new program outside of sanitary surveys that is no less stringent than federal regulations and involves identifying and addressing significant deficiencies in cybersecurity practices at

[8] NIST Computer Security Resource Center, https://csrc.nist.gov/glossary/term/ics
[9] 40 CFR § 142.16(b)(1)-(3) and (o)(1)-(2)
[10] 40 CFR § 142.16(o)(2)(iv)

PWSs.[11] States retain their existing flexibility with sanitary surveys in how they evaluate PWSs, identify significant deficiencies, and require PWSs to address significant deficiencies.

This interpretation applies to all states, territories, and tribes that have jurisdiction over PWSs. During any period when a state, territorial, or tribal government does not have primary enforcement responsibility pursuant to Section 1413 of the Safe Drinking Water Act (SDWA), the term "state" means the Regional Administrator, U.S. EPA. As indicated above, the use of "state" in this guidance encompasses this definition.

3.0 What approaches can states follow to include cybersecurity in PWS sanitary surveys?

EPA recognizes that several states have already established programs to evaluate PWS cybersecurity practices and to assist PWSs with protecting against cyber threats. Other states may have less capacity to assist communities sufficiently in building protections against cyber threats. To account for the differences among states in their capacity and capability, EPA is providing information on different approaches states could employ to evaluate cybersecurity at PWSs. In addition, states may want the flexibility to use different approaches based on the circumstances of individual PWSs, as well as to transition from one approach to another as capacity and capability change over time.

3.1. Option 1: PWS self-assessment or third-party assessment of cybersecurity practices

States that have or establish the requisite authority may require PWSs to conduct a self-assessment of cybersecurity practices for the purpose of identifying cybersecurity gaps (i.e., the absence of recommended cybersecurity practices or controls or presence of vulnerabilities).

Option 1.a. Self-Assessment. PWSs could conduct the assessment using a government or private-sector method approved by the state, such as those from the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA),[12] National Institute of Standards and Technology (NIST),[13] American Water Works Association

---

[11] Under SDWA Section 1413, 42 U.S.C. § 300g-2, states with primary enforcement responsibility (primacy) do not have to adopt drinking water regulations identical to EPA's national primary drinking water regulations. Rather, primacy states must adopt drinking water regulations that are "no less stringent" than EPA's national primary drinking water regulations, meaning that these states have a certain degree of flexibility in attaining and maintaining primacy.

[12] CISA *Cyber Resilience Review*, https://www.cisa.gov/uscert/resources/assessments

[13] NIST *Cybersecurity Framework*, https://www.nist.gov/cyberframework

(AWWA),[14] International Organization for Standardization (ISO),[15] and International Society of Automation/International Electrotechnical Commission (ISA/IEC).[16] In Section 5 and Appendix A of this guidance, EPA has provided an optional Checklist that PWSs (or states) may use to conduct an assessment of recommended cybersecurity practices and controls.

Option 1.b. Third-Party Assessment. Alternatively, a PWS could undergo an assessment of cybersecurity practices by an outside party, such as EPA's Water Sector Cybersecurity Evaluation Program[17] or another government or private sector technical assistance provider approved by the state. EPA is expanding its capacity to assist states and PWSs with conducting assessments.

Under Options 1.a and 1.b, the cybersecurity assessment for the PWS, whether it is a self-assessment or one conducted by a third party, should be completed prior to the sanitary survey, made available to state sanitary surveyors, and then updated to reflect changes in cybersecurity practices and/or operational technology prior to subsequent sanitary surveys. During the sanitary survey, the state surveyor should confirm completion of the assessment and determine whether identified cybersecurity gaps are significant deficiencies. As described in Section 7, this guidance provides examples and recommendations for states to consider when identifying a cybersecurity significant deficiency. Further, states and PWSs may consult with EPA for technical assistance once cybersecurity gaps are identified.

States may also require PWSs to develop follow-on risk mitigation plans to address cybersecurity gaps identified during the assessment, specifically including any significant deficiencies as designated by the state. The risk mitigation plan would list planned mitigation actions and schedules. The state would review the risk mitigation plan during the sanitary survey, ensure that the PWS is taking necessary steps to address any significant deficiencies as designated by the state, and offer to identify additional resources PWSs could use to address those gaps.

PWSs should complete the risk mitigation plan prior to their sanitary survey and update it, as necessary, prior to subsequent sanitary surveys. This guidance includes recommended actions for addressing cybersecurity gaps, and EPA offers a template for a risk mitigation

---

[14] AWWA, *Cybersecurity Assessment Tool and Guidance*, https://www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance

[15] ISO, *27001 Information Security Management*, https://www.iso.org/isoiec-27001-information-security.html

[16] ISA/IEC, *62443 series of standards*, https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

[17] EPA *Water Sector Cybersecurity Evaluation Program*, https://www.epa.gov/waterriskassessment/forms/epas-water-sector-cybersecurity-evaluation-program

plan at https://www.epa.gov/waterriskassessment/epa-cybersecurity-best-practices-water-sector. The template includes fields for a PWS to describe the planned mitigation action, target completion date, responsible party, current status, and explanatory notes. EPA technical assistance is also available to help states and PWSs regarding cybersecurity risk mitigation actions and plans.

3.2. Option 2: State evaluation of cybersecurity practices during the sanitary survey

States could choose to have surveyors evaluate cybersecurity practices directly during a sanitary survey of a PWS to identify cybersecurity gaps and determine if any of those gaps should be designated as significant deficiencies. This approach is consistent with how states conduct sanitary surveys for other components of PWS operations. Under this option, the state, rather than the PWS or a third party, would conduct the cybersecurity assessment and would direct the PWS to address any significant deficiencies that the state identifies. EPA training and technical assistance on evaluating cybersecurity in PWS sanitary surveys are also available to assist states that take this approach.

3.3. Option 3: Alternative state program for water system cybersecurity

Several states have programs under which PWSs assess for cybersecurity gaps (which might be called "security gaps," "vulnerabilities," or their equivalent) in their current practices that could impact safe drinking water and subsequently implement controls to address those gaps. For example, a state homeland security agency may have a cybersecurity program covering all critical infrastructure in the state. Another example is a state emergency management agency that conducts the cybersecurity assessment for the PWS instead of or in collaboration with the state agency responsible for the PWS supervision program.

States that currently have or that develop such programs may use these programs as alternatives to including cybersecurity in PWS sanitary surveys. PWSs serving rural communities with populations of less than 10,000 can utilize U.S. Department of Agriculture (USDA) Rural Development (RD) funded technical assistance providers. These communities may also already have requirements to complete cybersecurity analysis as part of loan and grant terms with USDA RD.

To be at least as stringent as a sanitary survey, state surveyors must ensure that the alternate state programs effectively identify cybersecurity gaps (or equivalent) through an assessment and that PWSs address any significant deficiencies as designated by the state. Further, the cybersecurity assessment performed under an alternative program must be conducted at least as often as the required sanitary survey frequency for the PWS (typically 3 or 5 years).

3.4. Changes to state recordkeeping and reporting

Because the memo does not change the *Code of Federal Regulations*, it does not require states to revise their approved state primacy programs.[18] If the state approves an agent other than the state to conduct the cybersecurity component of a sanitary survey at a PWS, as described under Option 1, the state must maintain a list of the approved agent(s).[19] States must include cybersecurity in their annual evaluation of the state's program for conducting sanitary surveys that states report to EPA.[20] For groundwater systems, states must maintain records of written notices of significant deficiencies and confirmation that a significant deficiency has been corrected.[21] States must report to EPA the date a groundwater system completed the corrective action.[22] States are not required to report the significant deficiency itself to EPA.

4.0 Technical support for cybersecurity in PWS sanitary surveys

In addition to this guidance, EPA is providing training and technical assistance as described below to help states and PWSs address cybersecurity in sanitary surveys. Further information on these resources, as well as additional material such as frequently asked questions (FAQs), fact sheets, and lists of potential funding programs, is available here: https://www.epa.gov/waterriskassessment/epa-cybersecurity-best-practices-water-sector. Section 4.3 below lists additional resources that can assist states and PWSs with evaluating cybersecurity and addressing deficiencies.

4.1. Training

In 2023, EPA plans to offer training for states and PWSs on evaluating cybersecurity in sanitary surveys. Like this guidance, the training will cover approaches to assess cybersecurity practices at PWSs, including identifying gaps and potential significant deficiencies, actions that PWSs could employ to close cybersecurity gaps, information protection, available technical assistance from EPA and other public and private-sector organizations, and potential funding.

Training will be delivered virtually with recorded versions available. Targeted training for states will also be offered in-person. This targeted training will be conducted separately for

[18] 40 CFR § 142.12
[19] 40 CFR § 142.14(a)(5)(ii)(F)
[20] 40 CFR § 142.15(c)(5)
[21] 40 CFR § 142.17(d)(i) and (iii)
[22] 40 CFR § 142.15(c)(7)(ii)

states in each EPA Region. For PWSs, training will be held nationally. For all trainings, EPA will strive to ensure state approval of Continuing Education Credits/Units (CECs/CEUs).

4.2. Technical assistance

EPA has established the *Cybersecurity Technical Assistance Program for the Water Sector.* Under this program, states and PWSs can submit questions or request to consult with a subject matter expert (SME) regarding cybersecurity in PWS sanitary surveys, such as identifying whether a cybersecurity gap is a significant deficiency or selecting appropriate risk mitigation actions. EPA intends for an SME to respond to the questioner within two business days. All assistance will be remote (phone or email as appropriate). The technical assistance service will not be an emergency line to report cyber incidents and it will not serve as a resource for cyber incident response or recovery efforts (users will be directed to the appropriate federal contact for these issues). Access this technical assistance service here: https://www.epa.gov/waterriskassessment/forms/epas-water-sector-cybersecurity-evaluation-program.

EPA's *Water Sector Cybersecurity Evaluation Program* is available to assess cybersecurity practices at PWSs. The assessment will follow the Checklist in this guidance document, *Evaluating Cybersecurity in PWS Sanitary Surveys* (Appendix A). Following the assessment, the PWS will receive a report with responses to Checklist questions that shows gaps in cybersecurity, including potential significant deficiencies. The PWS should provide this report to the state to review during the sanitary survey, as discussed under Option 1 in Section 3, above. To participate in this program, a PWS must register at https://www.epa.gov/waterriskassessment/forms/epas-water-sector-cybersecurity-evaluation-program.

4.3. Additional resources

Additional technical and financial resources that can help states and PWSs with assessing cybersecurity during sanitary surveys are listed below.

Technical resources

- Section 6 of this guidance lists examples of government and private sector methods in addition to EPA's that may be used to evaluate cybersecurity practices at PWSs and identify actions to address cybersecurity gaps.
- The NIST *Cybersecurity Framework*[23] is a comprehensive voluntary framework based on existing standards, guidelines, and practices for reducing cyber risks to critical

[23] https://www.nist.gov/cyberframework

infrastructure. NIST offers guidance and resources to assist critical infrastructure owners and operators with using the *Cybersecurity Framework* to manage their cyber risks.

- DHS CISA is a primary source of resources for critical infrastructure cybersecurity. CISA offers a broad array of tools, guidance, and services to strengthen the security and resilience of critical infrastructure facilities against cyberattacks.[24] For example, CISA products can help PWSs to identify cybersecurity vulnerabilities, develop proactive mitigation strategies that lower the cybersecurity risk of operational technology, and take steps to counter pervasive threats like ransomware.
- CISA Cybersecurity Advisors (CSAs), who are in the ten CISA regional offices, [25] offer cybersecurity assistance to critical infrastructure owners and operators and state, local, tribal, and territorial governments. CSAs act as liaisons to CISA cyber programs, along with other public and private resources. CSAs can assist with cyber preparedness, assessments and protective resources, partnership in public-private development, and cyber incident coordination and support.
- The USDA RD Circuit Rider program provides technical assistance, including cybersecurity analysis, to rural water systems serving 10,000 people or less. [26] Rural water system officials may also request assistance from their local USDA Rural Utilities Service office or from their National Rural Water Association (NRWA) State Association. Circuit Riders provide service in all states and territories.
- The Water Information Sharing and Analysis Center (ISAC)[27] is a source for data, case studies, and analysis related to water security threats, including cyber-crime, and provides resources to support response, mitigation, and resilience initiatives.
- The Multi-State ISAC supports information sharing to improve the overall cybersecurity of state, local, tribal, and territorial governments, assists cyber incident response and remediation, and issues advisories with actionable information for improving cybersecurity.[28]

---

[24] https://www.cisa.gov/cybersecurity

[25] https://www.cisa.gov/cisa-regions

[26] hhttps://www.rd.usda.gov/programs-services/water-environmental-programs/circuit-rider-program-technical-assistance-rural-water-systems

[27] https://www.waterisac.org/

[28] https://www.cisecurity.org/ms-isac

- Water sector private associations, including the AWWA[29] and NRWA[30] offer cybersecurity education, guidance, and methods to assess cybersecurity risks and prioritize cybersecurity enhancements that are targeted specifically to PWSs.

Financial resources

- EPA manages the Drinking Water State Revolving Fund (DWSRF) loan fund and set-asides, which may be used to support state programs and communities with cybersecurity controls.[31]
- EPA's Midsize and Large Drinking Water System Infrastructure Resilience and Sustainability Program is a new grant program for public water systems serving more than 10,000 people to support projects that increase resilience to natural hazards, cybersecurity vulnerabilities, or extreme weather events.
- The USDA Rural Utilities Service Water and Environmental Programs provide loans, grants, and loan guarantees, as well as technical assistance to PWSs in rural communities of 10,000 people or less for infrastructure and infrastructure improvements, which include cybersecurity upgrades.[32]
- The DHS State and Local Cybersecurity Grant Program managed jointly by CISA and the Federal Emergency Management Agency (FEMA) helps state, local, and territorial governments across the country address cybersecurity risks and threats to information systems that they own or that are operated on their behalf.[33,34]

5.0 EPA Cybersecurity Checklist for Public Water System Sanitary Surveys

5.1. What is the purpose of this Checklist?

EPA's Checklist (Appendix A) provides a method to evaluate the cybersecurity of operational technology, including information technology networks that are connected to the operational technology, at a PWS during a sanitary survey. The EPA Checklist questions and recommended actions to address deficiencies are extracted directly from the CISA *2022 Cross-Sector Cybersecurity Performance Goals.*[35] In the EPA Checklist, the Cybersecurity

[29] https://www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance
[30] https://nrwa.org/issues/cybersecurity/
[31] https://www.epa.gov/sites/default/files/2019-10/documents/cybersecurity_fact_sheet_final.pdf
[32] https://www.rd.usda.gov/programs-services/water-environmental-programs
[33] https://www.cisa.gov/cybergrants
[34] https://www.epa.gov/system/files/documents/2022-12/221121-SLCGP_508c.pdf
[35] https://www.cisa.gov/cpg

Performance Goals (CPGs) are written in a simplified question format to facilitate their use in evaluating a PWS.

The EPA Checklist questions are intended to identify cybersecurity gaps or potential vulnerabilities in current cybersecurity controls and practices. PWSs are encouraged to use the resources and technical assistance in the fact sheets in Appendix B of this guidance to address these gaps and reduce the risk that a cyberattack may compromise their operations.

A negative response to a checklist question is not, by itself, intended to indicate a significant deficiency at a PWS. Potential significant deficiencies are suggested in Section 7 of this guidance. The state is responsible for determining whether to designate a cybersecurity gap as a significant deficiency. In general, states should allow PWSs sufficient time to correct cybersecurity gaps identified in assessments and only consider issuing a significant deficiency where a PWS fails to correct a critical vulnerability.

5.2. The Checklist

The Checklist is provided in Appendix A.

6.0 Recommended alternatives to the EPA Checklist

The use of the EPA Checklist described in Section 5 and provided in Appendix A of this guidance during a sanitary survey is optional. Alternatively, the cybersecurity evaluation during a PWS sanitary survey may be conducted with other government or private-sector assessment methods approved by the state, such as those from CISA,[36] NIST,[37] AWWA,[38] ISO,[39] and ISA/IEC.[40]

7.0 Potential significant deficiencies

A "significant deficiency" as determined by the state[41] during a PWS sanitary survey is a deficiency that will cause the state to take enforcement action if it is not corrected within a designated schedule.

---

[36] CISA *Cyber Resilience Review*, https://www.cisa.gov/uscert/resources/assessments

[37] NIST *Cybersecurity Framework*, https://www.nist.gov/cyberframework

[38] AWWA, *Cybersecurity Assessment Tool and Guidance*, https://www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance

[39] ISO, *27001 Information Security Management*, https://www.iso.org/isoiec-27001-information-security.html

[40] ISA/IEC *62443 series of standards*, https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

[41] Includes tribes, territories, and EPA Regions when exercising primary enforcement authority for a public water system.

Section 2 presents EPA's regulatory definition of "significant deficiency" and applies this definition to cybersecurity in the context of a PWS sanitary survey (the absence of a control or practice that has a high risk of being exploited to compromise an operational technology asset used in the treatment or distribution of drinking water). Below, EPA suggests specific cybersecurity gaps from the Checklist shown in Appendix A for consideration by states as potential significant deficiencies. To select these gaps, EPA considered the following factors:

- High risk and history of exploitation in the water sector or other critical infrastructure sectors through widely used tactics, techniques, and procedures for cyberattacks,
- Technically feasible for most PWSs to address without significant capital expenditures, and
- Near-term implementation timeframe to correct.

States retain their existing authority and discretion to determine when a cybersecurity gap identified during a sanitary survey or equivalent alternate process should be designated as a significant deficiency. States also approve the actions and timing for PWSs to address significant deficiencies. As noted above, states may allow PWSs sufficient time to address cybersecurity gaps identified in assessments and only issue a significant deficiency where a PWS fails to correct a critical vulnerability.

The potential significant deficiencies suggested below are listed with their corresponding number from EPA Checklist provided in Appendix A, which aligns with the CISA *2022 Cross-Sector CPGs*.[42]

Account Security

- PWS does not change default passwords on operational technology (OT) assets when feasible OR implement compensating controls (e.g., segmentation or isolation of the asset, increased security event monitoring) when changing the default password for OT assets is infeasible. (Checklist /CPG 1.2)
- PWS does not use multi-factor authentication for remote access to OT networks. (Checklist/CPG 1.3)
- PWS does not require a minimum length for passwords. (Checklist/CPG 1.4)
- PWS does not revoke access credentials to PWS networks when an employee departs, or when a previously authorized user no longer requires access. (Checklist/CPG 1.7)

[42] https://www.cisa.gov/cpg

Device Security

- PWS does not maintain an updated inventory of all its OT assets (including all connected information technology (IT) assets). (Checklist/CPG 2.3)
- PWS does not maintain configuration documentation of its OT and IT assets. (Checklist/CPG 2.5)

Governance and Training

- PWS does not have a named role/position/title that is responsible for all PWS cybersecurity activities. (Checklist/CPG 4.1)
- PWS does not provide annual cybersecurity training for all staff. (Checklist/CPG 4.3)

Vulnerability Management

- PWS does not mitigate known vulnerabilities by installing firmware and software patches in a risk-informed timespan (critical or most exposed assets first) OR implement compensating controls (e.g., segmentation or isolation of the asset, increased security event monitoring) where patching is infeasible. (Checklist/CPG 5.1)
- PWS has not eliminated all OT asset connections to the public Internet unless explicitly required for operations. (Checklist/CPG 5.5)

Supply Chain/Third Party

- PWS does not include cybersecurity requirements and questions in its procurement documents for OT assets and services, which are then evaluated as a part of vendor selection (Checklist/CPG 6.1).
- PWS does not stipulate in its procurement documents that vendors and/or service providers shall notify the PWS of security incidents and confirmed vulnerabilities in a timely manner. (Checklist/CPG 6.2/6.3).

Response and Recovery

- PWS does not maintain an OT cybersecurity incident response plan. (Checklist/CPG 7.2)
- PWS does not backup all systems necessary for operations (e.g., network configurations, programmable logic controller [PLC] logic, engineering drawings) on a regular schedule. (Checklist/CPG 7.3)
- PWS does not store the backups separately from the source systems. (Checklist/CPG 7.3)

- PWS does not maintain updated documentation (e.g., drawings) of connections among all network components across OT networks (i.e., network architecture or topology). (Checklist/CPG 7.4)

The numbered fact sheets in this guidance (Appendix B) have information that can help PWSs resolve significant deficiencies by implementing the described cybersecurity controls.

8.0 How should states protect sensitive information on PWS cybersecurity?

Withholding from public disclosure information about specific cybersecurity practices and vulnerabilities at PWSs may be necessary due to the potential for this information to be exploited to facilitate a cyber intrusion or attack on the PWS.

In some cases, sanitary surveys are performed by EPA Regional Offices as the primacy agency for a particular state or area (e.g., Wyoming, the District of Columbia, most Indian Tribes). EPA may also perform cybersecurity assessments through the Water Sector Cybersecurity Evaluation Program (see Section 3.1). The Agency plans to assert applicable Freedom of Information Act (FOIA) exemptions to withhold sensitive portions of any sanitary survey report or PWS cybersecurity assessment held by EPA, including portions that deal with a PWS's cybersecurity practices if such a report is requested under FOIA. Applicable exemptions under FOIA for withholding such information may include Exemption 4 (confidential business information or CBI) and Exemption 7(f) (law enforcement records whose disclosure could reasonably be expected to endanger the life or physical safety of any individual).

For sanitary surveys conducted by a state, tribal, or territorial government, the applicable laws of the government entity that holds the report will govern the withholding of sensitive cybersecurity information from public disclosure. Most states have adopted information protection laws like FOIA under state law,[43] and EPA recommends that states withhold such sensitive information if requested to the extent allowable under state law. State requirements for reporting information to EPA related to evaluating cybersecurity in sanitary surveys are discussed in Section 3.4 above.

The addendum to the memo includes recommendations to states on potential approaches to identify and segregate cybersecurity information in sanitary survey reports that should be withheld from public disclosure. For example, states concerned about their authority to

[43] AWWA, *Protecting the Water Sector's Critical Infrastructure Information, Analysis of State Laws*, https://www.awwa.org/Portals/0/AWWA/Government/ProtectingtheWaterSectorsCriticalInfrastructureInformation.pdf

withhold sensitive cybersecurity information from public disclosure may take the following steps, if consistent with applicable state law:

- Sanitary surveyors may leave assessments of cybersecurity practices, the identification of cybersecurity gaps, mitigation plans, and other sensitive information with the PWS. The state would not hold this information.
- Official surveyor reports could be limited to confirming that the cybersecurity assessment was performed, indicating whether gaps were identified including significant deficiencies, and listing the schedule for corrective actions if needed. Information on specific gaps and significant deficiencies would be left with the PWS (not included in the state report or otherwise held by the state). The state surveyor would review progress in correcting significant deficiencies during virtual or onsite follow-ups.
- Where allowed, surveyors could keep detailed notes on PWS cybersecurity vulnerabilities and related information in internal, non-public documents that are not subject to public disclosure requirements.

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.

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.

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?

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.

[44] Under the Cyber Incident Reporting for Critical Infrastructure Act of 2022, CISA will establish procedures that may apply to public water systems. This recommendation will be revised as necessary when those procedures are issued.

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.

APPENDIX B: Checklist Fact Sheets

Account Security: Detection of Unsuccessful (Automated) Login Attempts

COST: **$**$$$ IMPACT: **HIGH** COMPLEXITY: **LOW**

1.1: Does the PWS 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.

Why is this control important?

A common technique that attackers use to break into OT and IT systems is to attempt to "guess" an actual username and password login combination. This attack can be accomplished by manually guessing an account's password, using a list of common passwords, or using a brute force technique. With this technique, an attacker uses a trial-and-error approach to systematically guess login credentials. The attacker submits combinations of usernames and passwords, generally using an automated, readily available password-cracking tool until the guess is correct. Blocking an attacker from future guesses after a specified number of incorrect guesses can stop these types of attacks. Without blocking login attempts, this attack will and can occur continuously until the attacker successfully cracks the password. A password cracker can run for hours, days, and weeks and eventually crack a password with brute force unless there is a policy that will stop it from happening.

Additional Guidance

- Enable systems to automatically notify (e.g., by a computer-generated alert) security teams or the System Administrator after a specified number of consecutive, unsuccessful login attempts in a short period (e.g., five failed attempts in under 2 minutes).
- Enable account lockout settings on applicable systems to prevent future login attempts for the suspicious account for a minimum time or until the account is re-enabled by the System Administrator.
- Log and store the alert information for analysis. Use sound logging procedures - a log should capture the event source, date, username, timestamp, source addresses, destination addresses, and any other useful information that could assist in a forensic investigation.

Implementation Tips

Depending on the version of Windows that a PWS uses, the System Administrator can use the Local Security Policy to restrict the number of login attempts. To access this feature, type "Local Security Policy" in the search box in the Start menu and click on the Local Security Policy App. Once the menu pane opens, click on "Account Policies" to adjust login attempts and lockout duration.

If a PWS utilizes a Microsoft Domain with many systems and user accounts connected to a single domain, it can manage these settings using Group Policy Objects (GPOs). The System Administrator can enable the Account Lockout Policy settings in the following location in the Group Policy Management Console: Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy. The Microsoft Windows Security Policy Settings Reference linked below provides additional details.

When implementing a login lockout threshold, ensure the account lockout threshold is set to an appropriate level based on the criticality of the system (generally between five to ten attempts). The selected level should provide leeway for operators to accurately input their credentials a few times but be robust enough to prevent most brute force attacks.

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See page 39, "Unsuccessful Logon Attempts" (control AC-7), for more information. *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

Center for Internet Security (CIS) Microsoft Windows Benchmark: This document describes how to implement preventative actions on Microsoft Windows-based systems. The section covering account lockout policy starts on page 50. Implementing detailed tracking is described on page 382.
https://www.cisecurity.org/benchmark/microsoft_windows_desktop

Microsoft Windows Security Policy Settings Reference: This page describes how to configure account lockout settings on Windows systems. *https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-threshold*

COST: **$**$$$ IMPACT: **HIGH** COMPLEXITY: **MEDIUM**

1.2: Does the PWS change default passwords?

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

Why is this control important?

Off-the-shelf hardware and software are designed for easy installation and use. Factory default settings often include simple, publicly documented passwords. Many times, these default passwords are identical (shared) among all systems from a vendor or within product lines. For these reasons, PWSs should change default passwords after initial testing, installation, and set-up are complete. Otherwise, attackers can easily obtain default passwords from a product's user manual and use these credentials to gain access to systems either locally or across the Internet if the target system is connected.

Additional Guidance

- Develop an enforced organization-wide policy and/or process that requires changing default vendor or manufacturer passwords for any hardware or software used at the PWS.
- While changing default passwords on a PWS's existing OT may require support from a qualified vendor or integrator and may not always be feasible, the PWS should change default credentials for all newly deployed hardware or software.

Implementation Tips

Many assets come with a default username and password that can be found in product documentation and on compiled lists available on the Internet. PWSs should review their existing asset inventory and identify any assets that could potentially have come with default passwords. These assets may include network hardware (e.g., network switches, wireless access points, network routers); communications assets (e.g., radios); OT assets (e.g., PLCs and HMIs); and software applications where the manufacturer or vendor installing the application at the PWS sets default passwords. The PWS should review the documentation for these assets, including instruction manuals and configuration guides (commonly available on the vendor's website), to identify any default usernames or passwords. Once the PWS identifies these username and password combinations, the System Administrator should attempt to login using these credentials, and if successful, determine if the Administrator can change them without impacting system operations. In instances where changing default passwords is not feasible, implement and document appropriate compensating security controls and monitor logs for network traffic and login attempts on those assets.

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: Provides a proactive and systemic approach to develop and make available a comprehensive set of safeguarding measures for all types of computing platforms. See control IA-5 (page 138) for more information on "Authenticator Management". *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

CISA Alert (TA13-175A): Issued in 2016, this alert describes why it is important to change the default password and provides mitigating actions. *https://www.cisa.gov/uscert/ncas/alerts/TA13-175A#:~:text=Attackers%20can%20easily%20identify%20and,to%20critical%20and%20important%20systems*.

COST: **$$**$$ IMPACT: **HIGH** COMPLEXITY: **MEDIUM**

1.3: Does the PWS require MFA wherever possible, but at a minimum to remotely access PWS OT networks?

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

Why is this control important?

MFA, also called two-factor authentication, requires PWS staff and other users to present at least two separate types of credentials when logging in to a PWS system. MFA can prevent an attacker who acquires a user password from accessing critical PWS networks. Credentials can be knowledge-based (like a password or PIN), asset-based (like a smart card or mobile phone), or biometric (like fingerprints). Credentials must come from two different categories – so entering two different passwords would not be considered MFA.

While MFA may not be necessary for all systems, it does provide a higher degree of security and should be used wherever possible. Higher-risk access such as authenticating remote users or vendors should be done by MFA as much as possible. Many remote access applications and virtual private network (VPN) systems offer this capability or can be set up to offer this capability by using a third-party tool.

Additional Guidance

- Use MFA to verify the identity of a user where possible. Common MFA methods include biometrics, smart cards, FIDO/CTAP (client to authenticator protocol) enabled hardware assets, or one-time passcodes sent to or generated by previously registered assets like a mobile phone.
- Within OT networks, enable MFA on all accounts and systems that the PWS can access remotely, including vendor/maintenance accounts, user, and engineering workstations, and HMI applications.

Implementation Tips

Review any use of remote access, particularly to OT systems, and identify if the PWS can enable MFA on the software used for this access. There are several applications that can assist with enabling multi-factor authentication at a PWS. Some of the most popular include TeamViewer and Microsoft 365 for Windows. The resources section below provides links for setup.

If the PWS cannot use MFA (such as some System Administrator, root, or service accounts), those accounts should use passwords that are unique to that one system and should not be accessible remotely where possible.

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See page 132 “Identification and Authentication” for more information on MFA. *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

Microsoft 365 Multi-factor Authentication Reference: This page describes how to configure multi-factor authentication settings on Microsoft 365 accounts. *https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide*

TeamViewer Authentication Reference: This page describes how to configure multi-factor authentication settings on the TeamViewer platform. *https://community.teamviewer.com/English/kb/articles/109255-enable-two-factor-authentication-enforcement-on-company-members*

COST: **$**$$$ IMPACT: **HIGH** COMPLEXITY: **LOW**

1.4: Does the PWS 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.

Why is this control important?

Using short passwords at a PWS is a significant security risk, as passwords play a vital role in preventing attackers from gaining access to users' accounts. Attackers use programs to guess user passwords, and a longer and more complex password is harder for an attacker to crack. Fully managing passwords includes enforcing password length, complexity (e.g., using upper- and lower-case letters), and ensuring users are following best practices for password security (e.g., no sticky notes with reminders stuck on monitors).

Additional Guidance

- Create a policy or set administrative controls that mandate a minimum password length (15 or more characters is recommended) for all password-protected OT and IT assets as feasible.
- In instances where minimum password lengths are not feasible, use compensating security controls (e.g., utilizing a single sign-on) and record all login attempts. Also, if computer assets cannot support longer passwords, prioritize them for upgrade or replacement.
- Utilize longer passwords or phrases as a password (e.g., "Iliketoeatapplesandbananas").

Implementation Tips

If a PWS does not currently have a policy document that addresses requirements for passwords including the minimum length and complexity, prepare one and ensure it is shared with all employees of the PWS.

For Windows-based OT and IT assets, depending on the version of Windows, the System Administrator can use the Local Security Policy to set a minimum length for passwords. To access this feature, type "Local Security Policy" in the search box in the Start menu and click on the Local Security Policy App. Once the menu pane opens, click on "Account Policies" and then "Password Policy" to adjust password length.

If a PWS utilizes a Microsoft Domain with many systems and user accounts are connected to a single domain, it can manage these settings using Group Policy Objects (GPOs). The System Administrator can configure the Password Policy settings in the following location in the Group Policy Management Console: Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy. The Microsoft Windows Password Policy Settings Reference linked below provides additional details.

For all other passwords on non-Windows-based assets, the Administrator should review existing passwords to ensure they meet the password policy where possible. These assets may include network hardware (e.g., network switches, wireless access points, network routers); communications assets (e.g., radios); OT assets (e.g., PLCs and HMIs); and software applications that use passwords to authenticate users.

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: Provides a proactive and systemic approach to develop and make available a comprehensive set of safeguarding measures for all types of computing platforms. See control AC-1 (page 39) for more information on "Access Control Policy and Procedures". *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

Password Guidance from NIST: NIST created a short video explaining password protection and guidance on implementing best practices. *https://www.nist.gov/video/password-guidance-nist-0*

CIS Control Password Policy Guide: The Center for Internet Security (CIS) provides a detailed breakdown of how to create and implement a password policy, specifics on password length start on page 7. *https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide*

CISA Security Tip (ST04-002): The U.S. Department of Homeland Security offers tips for effective passwords. *https://www.cisa.gov/uscert/ncas/tips/ST04-002*

Microsoft Windows Password Policy Settings Reference: This page describes how to configure password policy settings on Windows systems.

COST: **$**$$$ IMPACT: **HIGH** COMPLEXITY: **LOW**

1.5: Does the PWS 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.

Why is this control important?

The misuse of administrative privileges is a primary method for attackers to get inside a network. In one such method, a workstation user logged in as an Administrator or privileged user is fooled into opening a malicious email attachment, downloading and opening a file from a malicious website, or simply surfing a website hosting attacker content that can automatically exploit browsers. If the victim is logged in as an Administrator, the attacker can then use this access to launch an attack, such as deploying ransomware or installing keystroke loggers, sniffers, and remote-control software to find passwords and other sensitive data. A second common technique used by attackers is an elevation of privileges attack by guessing a password for a System Administrator. If a PWS loosely and widely distributes administrative passwords or sets them identical to passwords used on less critical systems, the attacker has a much easier time gaining full control of a system.

Additional Guidance

- A PWS should maintain an updated list/inventory of all Administrator accounts.
- Ensure that all users with administrative account access use a dedicated or secondary account for their administrative activities. This account should only be used for those administrative activities and not Internet browsing, email, or similar day-to-day activities.
- Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access these tools.
- Set up systems to create a log entry and issue an alert when the PWS adds to or removes an account from any group that has administrative privileges. Do the same for any unsuccessful logins to an administrative account.

Implementation Tips

Review all OT and IT user accounts to determine which ones are currently set as “Standard User” or “Administrator.” For those accounts that are currently set as Administrator, review whether that user requires Administrator privileges for his/her duties. If not, the PWS should downgrade the user to a Standard User account. If they do require Administrator privileges, but do not currently have a Standard User account for day-to-day functions, the PWS should create a separate Standard User account for that individual for day-to-day use.

The PWS should restrict use of the Administrator-level account to those individuals with a need for privileged access and only used for privileged functions.

For a PWS that uses Windows, there are five ways to find out what account type a user has (see Resource linked below). Knowing the account type for each user allows the PWS to determine whether there is a need to change a user's account type to allow or restrict additional privileges to perform administrative tasks.

A PWS can also change the level of an account in a common operating system by going to "Settings > Accounts > Family & Other Users", selecting the account in question, clicking on "Change Account Type", and selecting either "Administrator" or "Standard User".

Resources

- **WaterISAC's 15 Cybersecurity Fundamentals:** Page 15 provides more information on separating accounts. *https://www.waterisac.org/system/files/articles/15 Cybersecurity Fundamentals %28WaterISAC%29.pdf*
- **NIST Standard 800-53 Access Control Policy and Procedures, AC-1:** Page 18 provides information regarding access control and access management. *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*
- **NIST Standard 800-82 Guide to Industrial Control System (ICS) Security:** Section 6.2.1.1 provides additional information on role-based access control for SCADA systems. *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf*
- **Windows Central:** Identifies five ways to identify the account type of users within a network on Windows. *https://www.windowscentral.com/how-determine-user-account-type-windows-10#determine_windows10_account_type_settings*

1.6: Does the PWS 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.

Why is this control important?

Using separate usernames and passwords for users of the OT and IT networks is an integral part of a defense-in-depth strategy. Typically, if an attacker can determine a user's login on one network, they will use that login information to try to access other accounts or networks. This technique can allow an attacker to move laterally across a PWS operating environment. Also, it may not raise any alarms if system monitoring does not recognize the activity as "new" in the operating environment and can lead to a PWS not noticing a security incident. Bad actors can also use the password recovery feature on an account to access any account that uses the same email address.

Additional Guidance

- Where feasible, never allow multiple users to share a single login or a single user to use the same login for both the OT and IT networks.

Implementation Tips

Develop a policy that requires individuals to use separate accounts for OT and IT. If the PWS has a single Windows Domain that covers OT and IT systems, then evaluate splitting that Domain into two to stop users from sharing accounts across system types. Where users already have separate accounts for OT and IT, encourage them to not use a common password for these accounts.

The two most common operating systems are Microsoft Windows and Linux. Both systems allow a System Administrator the ability to manage accounts and account credentials for each end user. As mentioned before, the ability to separate end-user accounts is critical to any defense-in-depth strategy. The resources below provide details on how to manage user accounts for each system.

Resources

Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies: Page 25 provides OT network account management information. Note: CISA uses the term industrial control system (ICS) to refer to an OT network.
https://www.cisa.gov/uscert/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

Managing User Accounts on Windows: Provides more information on how to manage user accounts on Windows. *https://learn.microsoft.com/en-us/windows-server-essentials/manage/manage-user-accounts-in-windows-server-essentials*

Managing User Accounts on Linux: Provides more information on how to manage user accounts on Linux. *https://www.makeuseof.com/user-management-linux-guide/*

1.7: Does the PWS 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.

Why is this control important?

Inactive accounts may appear harmless, but they pose serious security risks when a PWS does not disable them or when accounts remain without password expiration limits. Attackers can use these accounts as the PWS may not notice their activities. Also, employees who leave the PWS could still use their login credentials to access network resources, which can be particularly risky if the employee left under strained circumstances.

Additional Guidance

- Terminate access to accounts and networks upon a change in a user's status making access unnecessary.
- Revoke access for terminated and voluntarily separated employees, vendors, contractors, and consultants as soon as possible.
- Evaluate staff's need for access upon promotion or other role change within the PWS and remove any access privileges no longer required for their new role.
- Establish an off-boarding procedure with human resources, contract managers, and OT and IT staff. The procedure should include an audit process to identify accounts that the PWS should disable and delete.
- Disable an individual's physical and cyber access to PWS facilities and systems as soon as the individual no longer requires access.

Implementation Tips

Developing a simple checklist that the PWS can use when a person either leaves the PWS or transitions into a new role at the PWS can be helpful. The checklist could include items such as returning any PWS-issued computer equipment like laptops, tablets, and smart phones, as well as deleting the individual's user accounts or changing privileges on user accounts as needed.

Resources

WaterISAC's 15 Cybersecurity Fundamentals: Page 17 provides more information on revoking credentials. *https://www.waterisac.org/system/files/articles/15 Cybersecurity Fundamentals %28WaterISAC%29.pdf*

COST: **$$**$$ IMPACT: **HIGH** COMPLEXITY: **MEDIUM**

2.1: Does the PWS require approval before new software is installed or deployed?

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

Why is this control important?

Users can utilize software to perform normal business activities or for malicious purposes intended to harm the computer system and/or business. An attacker may disguise malicious software as normal software to mislead a user into installing it, such as advertising legitimate features without disclosing malicious features or by mimicking the style and/or web address of a reputable vendor's download portal. An attacker can even compromise a legitimate vendor's software via a supply chain attack (e.g., SolarWinds Attack, 2020).

If a PWS employee intentionally or unintentionally installs malicious software, the PWS could be vulnerable to system breach, disruption, or damage. Permitting only approved software on PWS assets, preferably installed by an Administrator, allows the PWS to ensure that software is free of malicious code prior to installation.

Additional Guidance

- Establish controls for PWS-issued computers and other assets to restrict the software that users can install.
    - Examples include restricting administrative privileges (i.e., only certain designated individuals can install software on a PWS's computers, such as a System Administrator) or only allowing approved software downloads.
- Implement a process that requires approval before users can install new software or software versions.
- Maintain a risk-informed list of allowed PWS software, including specification of approved versions where technically feasible.

Implementation Tips

A PWS can manage software made available to staff through a download portal on each asset (e.g., Windows Software Center) or more simply from a list of approved software. To install new software, a PWS employee should submit a request to the OT/IT personnel or the System Administrator justifying the operational need for the new software.

Resources

GAO-22-104746 - Federal Response to SolarWinds and Microsoft Exchange Incidents: See the "What GAO Found" section for more information on the 2020 SolarWinds Supply Chain Attack. *https://www.gao.gov/products/gao-22-104746*

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control CM-11 (page 112) for more information on "User-Installed Software". *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

Microsoft Learn - Software Center User Guide: See this resource for more information on how to plan for and configure Microsoft Software Center. *https://learn.microsoft.com/en-us/mem/configmgr/apps/plan-design/plan-for-software-center?source=recommendations*

COST: **$**$$$ IMPACT: **MEDIUM** COMPLEXITY: **LOW**

2.2: Does the PWS 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.

Why is this control important?

Macros (i.e., embedded code) are software instructions contained within other files, such as Microsoft Office Word documents or Excel spreadsheets. Having these macros in a file can be helpful by automating repetitive tasks or updating data from online sources. However, attackers often use these macros to execute malicious code, download malware and viruses, or steal data.

An attacker can deliver a file with malicious macros to a PWS employee as an attachment to a phishing email. If the employee downloads the file, the macro within the file can leave the PWS's computer system vulnerable to breach, disruption, or damage. By disabling macros by default, a PWS can reduce the risk from executable code.

Additional Guidance

- When necessary for critical purposes, a PWS may enable macros on specific assets.

Implementation Tips

While a user can change this setting locally on individual assets, the PWS should implement it organization-wide through a system-enforced policy.

The PWS should have a policy in place for authorized users to submit a request to enable macros. This request should justify the operational need for enabling macros so that the relevant OT/IT personnel or System Administrator can make their decision to allow or disallow the request based on the potential risk to PWS operations.

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control SC-18 (page 311) for more information on managing macros, referred to as "Mobile Code". *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

Microsoft Learn - Block macros from running in office files from the Internet: See this resource for information on configuring Windows to block macros from the Internet. *https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked#block-macros-from-running-in-office-files-from-the-internet*

COST: **$$**$$ IMPACT: **HIGH** COMPLEXITY: **MEDIUM**

2.3: Does the PWS 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.

Why is this control important?

A PWS cannot protect or secure what it does not know it has. An accurate inventory of both OT (e.g., SCADA, PLCs, HMIs) and IT (e.g., office computers, network switches, servers) technology assets is a critical part of PWS cybersecurity. Once a PWS knows what assets it has, it can make necessary cybersecurity improvements on the OT and IT networks.

A PWS needs to understand what assets are on its SCADA, communications, and business systems. An accurate inventory will improve the PWS's knowledge of their assets, help it find any vulnerabilities in these assets, and help the PWS more easily respond to cyberattacks.

Additional Guidance

- Based on the review, update out-of-date records for known assets, add previously unknown assets to the inventory, and delete any assets from the list that the PWS no longer uses.
- Ensure the list identifies physical assets and also includes details for the assets, including how they are connected, what data they share, and who at the PWS (or what vendor) works with the asset.

Implementation Tips

There are several methods for identifying and inventorying assets, and the best approach will likely be a combination of physical inspection, passive scanning, active scanning, and configuration (set up) analysis. It is important to have this information to prepare for or respond to a cyberattack; however, it would also be valuable to an attacker so it should be protected accordingly.

Identifying and inventorying assets is an important first step for a PWS to take to know their assets. PWS should know what assets they have, how those assets are configured (see Factsheet 2.5), and how those assets are connected (see Factsheet 7.4).

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control CM-8 (page 107) for more information on "System Component Inventory". *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

SANS Institute Industrial Control System (ICS) Security Blog post "Know Thyself Better than the Adversary – ICS Asset Identification and Tracking": Provides information on asset identification and tracking. *https://www.sans.org/blog/know-thyself-better-than-the-adversary-ics-asset-identification-and-tracking/*

WaterISAC's 15 Cybersecurity Fundamentals: See the section on page 7, "Perform Asset Inventories" for additional information. *https://www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20%28WaterISAC%29.pdf*

COST: **$$$**$ IMPACT: **HIGH** COMPLEXITY: **HIGH**

2.4: Does the PWS prohibit the connection of unauthorized hardware (e.g., USB drives, 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.

Why is this control important?

Although cyberattacks coming from the Internet receive most of the attention, even if a PWS does not connect a network to the Internet (e.g., an "airgap"), it could still be vulnerable to attacks from direct connections. For example, if an employee or vendor uses a Universal Serial Bus (USB) drive or third-party laptop outside the PWS and then connects it to the PWS network, they may introduce malware onto the PWS's OT or IT systems (either intentionally or unintentionally).

Connecting a malicious USB asset to the PWS network can lead to system breach, disruption, or damage. The most well-known example of an attacker using a USB to damage an industrial plant is Stuxnet, the first publicly known malware designed to target OT systems. Only allowing authorized assets to connect to PWS networks helps stop attackers from getting into or stealing data from those networks.

Additional Guidance

- Disable AutoRun features that grant automatic access to removable media (e.g., USB drives) when connected to a computer.
- Allow access to physical connection ports on computers only through approved exceptions.

Implementation Tips

PWSs can stop the use of unauthorized assets by using physical cages to cover computer ports, through administrative policies (less effective), or by disabling technical permissions through an organization-wide policy within Microsoft Windows. If a PWS allows users to connect external assets to their systems, the PWS should check the assets for malware prior to connecting them. PWSs can generally configure anti-virus software to automatically scan external drives such as USBs when a user inserts them.

If necessary, establish an administrative process where a user can request an exception to using an external asset by justifying the operational need. The relevant OT/IT personnel or System Administrator will need to weigh the operational need against the potential security risk to the PWS's computer system(s).

Resources

MITRE ATT&CK - Stuxnet: See “Replication Through Removable Media” for more information on Stuxnet’s spread. *https://attack.mitre.org/software/S0603/*

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control MP-7 (page 176) and SC-41 (page 326) for more information on “Media Use” and “Port and I/O Device Access”. *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

Microsoft Learn - Enabling and Disabling AutoRun: See the section on “Using the Registry to Disable AutoRun” for more information. *https://learn.microsoft.com/en-us/windows/win32/shell/autoplay-reg#using-the-registry-to-disable-autorun*

COST: **$$**$$ IMPACT: **HIGH** COMPLEXITY: **MEDIUM**

2.5: Does the PWS 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.

Why is this control important?

While a PWS may know the physical assets that exist on its computer networks from performing an asset inventory (see Factsheet 2.3), understanding the configuration (i.e., settings) of its assets is important as well. Attackers often exploit vulnerabilities (i.e., weaknesses) that only exist in certain versions or settings of the software and firmware used to control assets. Therefore, a PWS should be aware of its asset configurations to know whether a newly found vulnerability could be used in an attack on its network.

Additionally, if an attacker changes asset configurations, wipes settings, or disables assets, well-maintained configuration documentation will allow the PWS to detect changes more easily, re-establish appropriate settings, and maintain or restore operations.

Additional Guidance

- Review and update configuration documentation on a regularly scheduled basis.

Implementation Tips

To fully document asset configurations, include the following details, as applicable: owner (e.g., Engineering Department), physical and network location, vendor, asset type, model, asset name, firmware and/or software versions, patch levels, asset configurations, active services (i.e., automated processes), communication protocols, network addresses (e.g., IP and MAC), asset value, and criticality to PWS operations.

To be efficient, a PWS can perform a review of its asset configuration at the same time as the asset inventory process detailed in Factsheet 2.3 and the network survey detailed in Factsheet 7.4. Configuration information is important to preparing for or responding to a cyberattack; however, it would also be valuable to an attacker, so the PWS should protect it accordingly.

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control family CM-1 (page 96) and control CM-6 (page 103) for more information on “Configuration Management” and “Configuration Settings”. *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

3.1: Does the PWS 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.

Why is this control important?

Logging is recording data about events that take place in a PWS's OT or IT systems. When responding to a cyberattack, having detailed logs will help the PWS and other investigators determine how and when an attacker was able to break into their systems, what areas they accessed, and if they breached any sensitive data. Regular reviews of these logs may also allow the PWS to detect an attacker before they are able to impact systems.

Additional Guidance

- Check logs regularly for both completeness and to ensure that all necessary information can be found in case of a cyberattack.
- If a log source (e.g., Windows Event Logging) is not active, notify the System Administrator or individual responsible for system security.
- If logs are not available for certain OT assets, collect information about network traffic and communications to and from these assets.

Implementation Tips

Log sources include but are not limited to network logins and logs from servers, end-user assets (e.g., desktops and laptops), networking equipment (e.g., routers and switches), applications/programs, Intrusion Detection System/Intrusion Protection Systems (IDS/IPS), firewalls, anti-virus software, Data Loss Prevention (DLP) tools, and Virtual Private Networks (VPNs).

If possible, PWSs should capture, review, and securely store logs from all these sources for future reference in the event of a cyberattack. At a minimum, PWSs should enable logging for critical servers, firewalls, and remote access tools such as VPNs. A review of the configuration manuals for any firewalls or remote access tools should provide instruction on how to configure and enable logging for these specific assets.

For Windows-based systems, the Windows "Event Viewer" application gives the PWS the ability to manually review security logs on an individual asset. To see an example security log in Windows, open the "Event Viewer" app. In the console tree, expand "Windows Logs", and then click "Security". The results pane lists individual security events. To see more details about a specific event, click the event in the results plane. The PWS can collect Windows Events from both servers and endpoints (e.g., desktops and laptops) on a central server for more efficient manual analysis using the Windows Event Collector. While this

method is an improvement over fully manual log review, it will not include logs from non-Windows assets and applications – providing an incomplete picture of PWS operations.

To overcome this issue, the PWS can use log aggregation software and Security Information Event Management (SIEM) systems to centrally collect logs from practically all sources, simplify reviewing logs, and target events of interest. In addition to having all logs in one place, these tools can also automate many steps of log analysis, making the PWS security team more effective and saving time in the process.

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control AU-2 (page 66) for more information on "Event Logging." *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

WaterISAC's 15 Cybersecurity Fundamentals: See page 31 for more information on "Logging and Auditing." *https://www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20%28WaterISAC%29.pdf*

Microsoft Learn – Windows Event Collector: See this resource for more information on setting up Windows Event Collector. *https://learn.microsoft.com/en-us/windows/win32/wec/windows-event-collector*

COST: **$$$**$ IMPACT: **HIGH** COMPLEXITY: **LOW**

3.2: Does the PWS 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.

Why is this control important?

Once a PWS collects security logs, it should store and protect the logs. This step is important because if an attacker compromises a system, they may modify or delete logs to destroy evidence and cover their tracks.

Without trusted log data to track what an attacker does on a PWS computer system, both detecting and responding to a cyberattack becomes much more difficult. The System Administrator won't know where the attacker went, what they did, or when they did it. This step helps to make sure that the PWS protects its security logs from unauthorized access and tampering.

Additional Guidance

- Store logs for a period that considers PWS policy, state regulations (if any), and cyber risk. A common log retention period is six months.
- Ensure security logs are part of the PWS's standard backup procedures so that the PWS can review the logs even if the source is no longer available.

Implementation Tips

Storing logs in a central system or database can be achieved using Security Information and Event Management (SIEM) systems, further covered in Factsheet 3.1. In addition to ease of log collection and analysis, SIEM tools also enable the System Administrator to set access permissions by user, referred to as Role-Based Access Control (RBAC). When storing logs in a central location with or without a SIEM tool, ensure that each user has an individual account to access log storage (i.e., SIEM Tool, Log Database, or Log Server).

Regardless of how the PWS stores the logs, it should back them up to a secondary storage location on a regular schedule. A common backup schedule is daily. Regulatory, operational, and technological requirements and constraints often determine log retention periods; however, a common log retention period is six months. A longer log retention period is generally better than a shorter one as responders will have more evidence to review when investigating a potential cyberattack.

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control family AU and AU-9 (page 74) for more information on "Audit and Accountability" and "Protection of Audit Information."
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

WaterISAC's 15 Cybersecurity Fundamentals: See page 31 for more information on "Logging and Auditing."
https://www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20%28WaterISAC%29.pdf

Microsoft Learn – Set up or customize server backup: See this resource for more information on how to configure backups for log storage locations.
https://learn.microsoft.com/en-us/windows-server-essentials/manage/set-up-or-customize-server-backup

3.3: Does the PWS 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.

Why is this control important?

Encryption is the process by which computers convert information (e.g., files, network traffic) from "plain text" that people can read into a coded message that they cannot read. This step is important, as attackers will often attempt to intercept messages to alter commands to OT assets and steal passwords or other sensitive information.

By using strong encryption when sending information, even if attackers can intercept a message, they will not be able to use the information as it will be unreadable. This step helps to maintain the confidentiality (i.e., secrecy) of sensitive information and the integrity (i.e., correctness) of OT and IT information.

Additional Guidance

- For OT computer systems, such as SCADA, use encryption for communications with remote or external assets.
- Update any weak or outdated data encryption software.

Implementation Tips

TLS and SSL are the most common encryption protocols that systems use for sending information and data, and PWSs can configure assets such as desktops and servers to send and receive encrypted messages using one of these protocols. TLS is a newer and more secure alternative to SSL and is generally the preferred encryption standard if feasible. A PWS should perform a review of the current encryption protocol that it uses, compare this protocol to current standards, and develop a plan for improvement if necessary and operationally feasible.

Configuration settings for encryption may be available for a variety of communications including remote access software, web-based HMI software, wireless communications (e.g., Wi-Fi), and radio communications. A PWS should encrypt and password-protect Wireless communications and avoid "open" (i.e., password-less) Wi-Fi networks. Virtual Private Networks (VPNs) for remote access into PWS systems and Cloud services for remote storage and application hosting will likely offer this capability by default.

Within Windows, the PWS can enable TLS via the Configuration Manager. If implementing TLS via Windows Configuration manager, make sure to start with clients/endpoints (desktops and laptops). If starting implementation at the server-level, it may cut off communication to client assets.

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control SC-8 (page 304) for more information on "Transmission Confidentiality and Integrity." *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

Microsoft Core Infrastructure Guide: See the links below for instructions on how to enable TLS 1.2 on clients (e.g., desktops and laptops) and servers via Windows Configuration Manager. *https://learn.microsoft.com/en-us/mem/configmgr/core/plan-design/security/enable-tls-1-2-client* ; *https://learn.microsoft.com/en-us/mem/configmgr/core/plan-design/security/enable-tls-1-2*

COST: **$$**$$ IMPACT: **HIGH** COMPLEXITY: **MEDIUM**

3.4: Does the PWS 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.

Why is this control important?

See Factsheet 3.3 for a description of the importance of general encryption.

This control is important, as attackers will often attempt to break into computer systems and databases to steal sensitive information and "case" the network for a future attack. Additionally, many ransomware cyberattacks also include extortion attempts whereby the attacker will steal a PWS's sensitive data and threaten to expose it on the Internet if a ransom is not paid. If the PWS encrypts data, the attacker will not be able to use it if stolen as it will be unreadable.

Additional Guidance

- Only allow access by authorized users.
- Update any weak or outdated data encryption software.

Implementation Tips

A PWS can implement encryption for stored data using BitLocker for drive encryption of servers and clients (desktops and laptops), as well as with Transparent Data Encryption (TDE) for database files. A PWS can encrypt and password-protect Individual sensitive files in Windows by right-clicking a file, selecting Properties -> Advanced -> "Encrypt contents to secure data". Cloud services for remote storage and application hosting will likely offer this capability by default.

To securely store and use credentials, a PWS can use a password management software (e.g., LastPass, 1Password) or other account management method. Password management software securely stores credentials, reduces the difficulty of remembering passwords, and simplifies the use of complex passwords.

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control SC-13 (page 308) and SC-28 (page 317) for more information on "Cryptographic Protection" and "Protection of Information at Rest".
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Microsoft Core Infrastructure Guide: See the links below for instructions on how to encrypt stored data via BitLocker Drive Encryption, Transparent Data Encryption (TDE) for databases, and individual file encryption. *https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/security/transparent-data-encryption;*

https://learn.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview;

https://support.microsoft.com/en-us/windows/how-to-encrypt-a-file-1131805c-47b8-2e3e-a705-807e13c10da7

COST: **$**$$$ IMPACT: **HIGH** COMPLEXITY: **LOW**

4.1: Does the PWS 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.

Why is this control important?

To prepare for and respond to cybersecurity threats effectively across the PWS, it is essential to create a top-down strategy, starting with the assignment of an overall cybersecurity "lead". The PWS can associate the "lead" responsibility with a current job position. The individual in the lead position should be responsible and accountable for planning, resourcing, and overseeing the execution of cybersecurity activities. The cybersecurity lead may undertake activities such as managing cybersecurity operations at the senior level, providing awareness training to employees, planning exercises (e.g., tabletop exercises), requesting and securing budget resources for cybersecurity activities such as vendor support, and reporting to the board or management on cybersecurity activities.

Additional Guidance

- Select a position within the PWS for the named role/position/title responsible for overall cybersecurity. The individual in this role should be different than the System Administrator if possible. This individual should be an employee of the PWS, and not a vendor or contractor, so that the PWS can hold them accountable for the duties they undertake.
- Establish clear tasks and duties for the cybersecurity lead and document them, such as adding these to an existing position description. Include diagrams and photos where necessary.
- Identify any critical staff that should assist the cybersecurity lead.

Implementation Tips

The person responsible as the overall cybersecurity lead does not need to be a cyber expert; however, some knowledge of how the PWS's OT and IT systems work would be helpful.

Ensure that the cybersecurity lead has sufficient training opportunities to effectively serve in the role. Include the execution of the individual's roles and responsibilities as cybersecurity lead in their performance reviews.

Resources

WaterISAC's 15 Cybersecurity Fundamentals: Page 25 provides information on creating a cybersecurity culture at a PWS, including executive and board engagement. *https://www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20%28WaterISAC%29.pdf*

NICCS's Workforce Framework for Cybersecurity (NICE Framework): This resource helps employers develop their cybersecurity workforce. Review the "Cybersecurity Management" module. *https://niccs.cisa.gov/workforce-development/nice-framework/specialty-areas/cybersecurity-management*

Cyber Essential Toolkit Courses: This toolkit is a set of modules designed to break down the CISA Cyber Essentials into manageable steps for a cybersecurity lead. *https://www.cisa.gov/publication/cyber-essentials-toolkits*

COST: **$**$$$ IMPACT: **HIGH** COMPLEXITY: **LOW**

4.2: Does the PWS 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.

Why is this control important?

In addition to an overall cybersecurity lead (see Factsheet 4.1), PWSs should assign a named role/position/title the responsibility as lead for OT-specific cybersecurity activities given the complexities of OT. The person who fills this "OT cybersecurity lead" role/position/title should have oversight and authority for all OT-specific cybersecurity and be responsible for planning, resourcing, and execution of all OT-specific cybersecurity activities.

Additional Guidance

- Select a position within the PWS for the named role/position/title responsible for OT cybersecurity. This OT cybersecurity lead could be the same role/position/title named in 4.1, a different role/position/title at the PWS, a municipal or county level role/position/title, or the role/position/title overseeing a designated OT vendor who provides cybersecurity services. The OT cybersecurity lead may be different than the System Administrator. The OT cybersecurity lead could be the same role/position/title responsible for overall OT operations.
- Establish and document clear tasks for the OT cybersecurity lead, such as adding these tasks to an existing position description. Include diagrams and photos where necessary.
- Identify any critical staff that should assist the OT cybersecurity lead.

Implementation Tips

The PWS employee responsible as the OT cybersecurity lead should have a good working knowledge of how the PWS configures, uses, and maintains its OT systems. For example, the PWS could name an employee who uses OT as part of their regular duties in the role/position/title.

If the OT cybersecurity lead will fully discharge their duties with no outside help, ensure that the PWS employee in this role has sufficient training opportunities to effectively carry out their responsibilities. Include in performance reviews the execution of the responsibilities of OT cybersecurity lead. If a vendor will serve as the OT cybersecurity lead, the PWS should include language to this effect in the service level agreement/contract.

Resources

NCCIC's ICS Cybersecurity for the C-Level: Provides examples of six cybersecurity risk oversight questions an OT cybersecurity lead should be asking about their organization's

environment and includes services and practical action steps specific to critical infrastructure. *https://www.cisa.gov/uscert/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_ICS_Cybersecurity_C-Level_S508C.pdf*

NICCS's Workforce Framework for Cybersecurity (NICE Framework): This resource helps employers develop their cybersecurity workforce. Review the "Cybersecurity Management" module. *https://niccs.cisa.gov/workforce-development/nice-framework/specialty-areas/cybersecurity-management*

COST: **$**$$$ IMPACT: **HIGH** COMPLEXITY: **LOW**

4.3: Does the PWS provide at least annual training for all PWS personnel that covers basic cybersecurity concepts?

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

Why is this control important?

To help create and maintain a culture of cybersecurity, a PWS should provide regular, basic cybersecurity training to all personnel. While cybersecurity covers many areas, there are certain basic security concepts that the PWS should regularly emphasize for general awareness and to promote better cyber practices. When PWSs train personnel regularly, those personnel are more likely to identify and respond quickly to a potential cyber incident or prevent one from occurring altogether. Regular training is critical as cybersecurity threats constantly evolve.

Additional Guidance

- Establish a schedule to conduct regular training for all PWS personnel that covers basic cybersecurity concepts. The frequency of the training should be once per year, at a minimum.
- Establish a policy that requires new employees to receive initial cybersecurity training within 10 days of onboarding. The training should consider the role of the new employee and cover basic security topics.

Implementation Tips

Develop an agenda for the training to cover basic cybersecurity concepts, such as phishing, business email compromise, password security, latest trends and threats in social engineering, and best cyber hygiene practices. Social engineering is a common way to exploit people via social media (e.g., Facebook) and human interaction (e.g., email) to gain sensitive information and access. Use training concepts that are familiar to PWS staff, including real examples based on the equipment and systems used by the PWS. For example, if the PWS issues a smart phone to the employee, include specific training related to smart phone security. Since all staff probably receive email, the training should always include cybersecurity best practices for reviewing and opening email.

Develop the training materials so they are easy to follow and for personnel to reference later. Update PowerPoint presentations, online learning modules, and handouts for each training. Provide links to additional resources where PWS personnel can learn more about the cybersecurity topics. To keep cybersecurity relevant and fresh, consider adding a short cybersecurity segment to PWS staff meetings and briefings to share a quick tip or information related to cybersecurity.

Staff that attackers commonly target, such as executives, executive assistants, engineers, SCADA staff, IT staff, operators, human resources, and finance personnel should receive

more specialized training. Many free training opportunities are available online and in person, including from CISA and NICCS (see resources below).

Resources

WaterISAC's 15 Cybersecurity Fundamentals: Page 25 provides information for creating a cybersecurity culture at a PWS, including providing cybersecurity awareness training to all PWS staff. *https://www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20%28WaterISAC%29.pdf*

NIST Standard 800-16 and 800-50 Building an Information Technology Security Awareness and Training Program: Provides guidance for building an IT security awareness and training program. *https://csrc.nist.gov/publications/detail/sp/800-50/final*; *https://csrc.nist.gov/publications/detail/sp/800-16/final*

NIST Standard 800-82 Guide to Industrial Control Systems Security: Section 6.2.2 on page 6-13 provides ICS training guidance. *https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final*

CISA Training: Provides no cost online training on a variety of cybersecurity topics. *https://www.cisa.gov/cybersecurity-training-exercises*

CISA Virtual Learning Portal: Provides no cost online training on a variety of cybersecurity topics. *https://www.cisa.gov/uscert/ics/Training-Available-Through-CISA#need*

NICCS Federal Virtual Training Environment (FedVTE) Cybersecurity Training: Provides no cost online cybersecurity training for state, local, tribal, and territorial government employees. *https://niccs.cisa.gov/education-training/federal-virtual-training-environment-fedvte*

Stop Ransomware.gov: This is the U.S. Government's official one-stop location for resources to tackle ransomware more effectively. *https://www.cisa.gov/stopransomware*

COST: **$**$$$ IMPACT: **HIGH** COMPLEXITY: **LOW**

4.4: Does the PWS 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.

Why is this control important?

The importance of regular basic cybersecurity training for all personnel is addressed in Factsheet 4.3. In addition, personnel who maintain or secure OT as part of their regular duties should receive OT specific cybersecurity training on at least an annual basis.

Additional Guidance

- Identify the PWS personnel who should receive more specialized OT-focused cybersecurity training. At a minimum, PWSs should provide this specialized training to personnel who use OT assets as part of their regular duties.

Implementation Tips

The PWS's designated OT vendor may be capable of conducting OT-focused cybersecurity training for the PWS.

Instead of one large training that covers many topics, a PWS should conduct multiple trainings scheduled periodically throughout the year to help break topics into short, digestible sessions.

Develop the training agenda and materials so they are easy to follow and reference later. The training should cover OT asset security, configurations, safety functions, incident response actions, and general operations. If the PWS can operate manually without the use of OT, consider adding training for manual operations. Manual operations may be an essential line of defense in keeping the PWS operational in the event of a cyberattack. There are many online training opportunities available for PWS personnel, including those from CISA and NICCS (see resources below).

Resources

CISA ICS Training: Provides no cost online training on a variety of OT security topics. *https://www.cisa.gov/uscert/ics/Training-Available-Through-CISA*

NIST Standard 800-82 Guide to Industrial Control Systems Security: Section 6.2.2 on page 6-13 provides ICS training guidance. *https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final*

NICCS Federal Virtual Training Environment (FedVTE) Cybersecurity Training: Provides no cost online cybersecurity training for state, local, tribal, and territorial government employees. *https://niccs.cisa.gov/education-training/federal-virtual-training-environment-fedvte*

SANS Institute - Premier Hands-on ICS Training: This fee-based training offers several courses designed to increase the cybersecurity skills of those who use OT/ICS at their PWS. *https://www.sans.org/cyber-security-courses/?focus-area=industrial-control-systems-security&msc=main-nav*

COST: **$**$$$ IMPACT: **MEDIUM** COMPLEXITY: **LOW**

4.5: Does the PWS 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.

Why is this control important?

To ensure a PWS meets all its cybersecurity needs, it is critical that both OT and IT personnel, including vendors, understand each other's cybersecurity drivers, challenges, needs, and goals. Since separate departments often use OT and IT systems and separate staff or vendors maintain them, PWSs frequently manage the security of these systems separately. This separation can lead to gaps in security, especially with interconnected OT and IT systems. Regular coordination and communication between OT and IT cybersecurity personnel can help develop a more comprehensive approach to PWS cybersecurity.

Additional Guidance

- Sponsor at least one collaborative meeting per year for OT and IT personnel. Finding a date and time that works for all parties can be difficult, so schedule the meeting well in advance. In-person meetings provide more relationship building opportunities.
- Develop an agenda in advance of the meeting to allow time for OT and IT personnel to prepare their discussion points. Topics can include new PWS OT/IT hardware, firmware, and software updates; changes in network architecture; reports on updated plans, policies, or procedures; changes in personnel; roles and responsibilities; planned future cybersecurity activities; and emerging cybersecurity threats.
- Record action items from the meeting, including personnel responsible, so that the PWS can check item status at regular intervals.

Implementation Tips

PWS vendor(s)/contractor(s) may require payment for their attendance at the meeting. The PWS should plan for this cost in its budget. The PWS can schedule the meeting on a day when the vendor(s)/contractor(s) would benefit from other onsite activities. For example, schedule the meeting for the same day the vendor(s) is(are) planning to be at the PWS to conduct regular system maintenance.

A cybersecurity drill, or tabletop exercise, is an impactful way to bring together both OT and IT personnel, practice existing plans, policies, and procedures, and address security gaps based on exercise lessons learned. Including a few social breaks in the exercise can allow for relationship building.

Resources

EPA Tabletop Exercise Tool: This tool helps PWSs to design their own exercises; a cybersecurity scenario is provided. *https://ttx.epa.gov/index.html*

CISA Tabletop Exercise Packages: These resources are designed to assist PWSs and others in conducting their own exercises. Note that under "Cybersecurity Scenarios" there is one for water systems. *https://www.cisa.gov/cisa-tabletop-exercise-packages*

COST: **$**$$ IMPACT: **HIGH** COMPLEXITY: **MEDIUM**

5.1: Does the PWS patch or otherwise mitigate known vulnerabilities within the recommended timeframe?

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

Why is this control important?

A vulnerability is a weakness in a piece of software or firmware running on a hardware asset. Vulnerabilities can come from mistakes in code or oversights in the software design process, or attackers may intentionally place vulnerabilities in software as a vendor writes the code (i.e., a supply chain attack). An exploit is either a set of actions or a piece of malicious code that attackers use against the vulnerability, helping them breach a computer system or damage an asset.

When a PWS discovers a vulnerability, the original creator of the software will generally work on a new version that does not contain the same weakness. Installing this software update is known as "patching" a system and upgrading to the new version prevents an attack from "exploiting" the known vulnerability. This control is important because it reduces the chances of attackers taking advantage of published vulnerabilities to breach a PWS's computer systems.

Additional Guidance

- For assets where patching is not feasible, apply compensating controls like segmentation (i.e., digitally separating the network into smaller pieces, each protected from the other) and enhanced monitoring (e.g., installation of network traffic monitoring tools).
- Acceptable measures either make the asset unreachable from the public Internet or reduce the ability of attackers to use the vulnerability in a cyberattack.

Implementation Tips

To adopt this control, a PWS can use their Asset Inventory (see Factsheet 2.3), Configuration Documentation (see Factsheet 2.5), and the resources below to identify vulnerabilities that exist in their system. For IT assets, automated updates and patches are often already enabled (e.g., Windows updates). But for OT assets, the PWS often disables automated updates and patches. Therefore, a PWS may need to manually apply updates and patches for OT assets based on availability and operational feasibility. If a patch is not available or would unacceptably disrupt PWS operations, a PWS can use mitigating controls such as Network Segmentation (see Factsheet 8.1).

To help PWSs stay aware of vulnerabilities, the U.S. federal government maintains several software vulnerability data resources and can send alerts about new entries to these databases. The most important is the Known-Exploited Vulnerability (KEV) database

published by DHS CISA, containing information about vulnerabilities that attackers are already using. Any vulnerabilities on the KEV should receive the highest degree of prioritization. The National Vulnerability Database (NVD) published by NIST contains information about all publicly known vulnerabilities. PWSs should also register to receive alerts and advisories from DHS on new vulnerabilities. If the PWS is a WaterISAC member, it will also receive cybersecurity threat notifications, including critical vulnerabilities.

To automate the process of identifying vulnerabilities, DHS CISA offers free services for Internet-facing systems (see Factsheet 5.4) and many vendors offer paid vulnerability scanning tools and services for internal computer systems. To aid in vulnerability identification, a PWS can use a vulnerability scanner in the IT network and a passive monitoring tool in the PWS OT network.

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control SI-2 (page 333) and RA-5 (page 242) for more information on "Flaw Remediation" and "Vulnerability Monitoring and Scanning". *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

DHS CISA Known-Exploited Vulnerabilities (KEV): See this resource for vulnerabilities that attackers have already exploited. *https://www.cisa.gov/known-exploited-vulnerabilities-catalog*

NIST National Vulnerability Database (NVD): See this resource for a list of publicly known vulnerabilities. *https://nvd.nist.gov/vuln/search*

DHS CISA Alerts: See this resource to sign up for email alerts from DHS CISA's National Cyber Awareness System regarding new vulnerabilities. *https://www.cisa.gov/uscert/ncas/alerts*

WaterISAC: See this resource for more information about the Water Information Sharing & Analysis Center (ISAC). *https://www.waterisac.org/*

5.4: Does the PWS 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.

Why is this control important?

A network perimeter is the secured boundary between the PWS's side of a network (the intranet) and the public Internet-facing side of the network. The perimeter contains the ports or "entrances" that attackers attempt to use to gain access to a PWS's intranet. If a PWS connects a port or service (i.e., program) to the Internet, then a pathway exists for a cyberattack and the PWS needs to implement security measures to address it.

The February 2021 breach of Oldsmar Florida's water facility is an example of an attack using Internet-facing remote access software (such as TeamViewer or Remote Desktop Protocol) to alter PWS operations. In the case of Oldsmar, attackers increased the amount of sodium hydroxide in drinking water to unsafe levels. Additionally, attackers have used Internet-exposed remote access software to introduce ransomware to a PWS SCADA computer. This control is important because closing ports and services to the public Internet helps prevent attackers from accessing the network.

Additional Guidance

- If a PWS connects external facing services (e.g., remote access, web hosting) to the public Internet, the PWS should implement appropriate compensating controls (e.g., firewalls, multi-factor authentication, or activity logging and monitoring) to prevent common forms of attack.

Implementation Tips

A PWS can search for Internet-exposed ports and services by using Shodan (a "search-engine" for Internet-facing assets) for assets on their network. Additionally, DHS CISA offers free vulnerability scanning services that scan for Internet-exposed services and alert the PWS of results.

Sometimes a PWS must connect and therefore expose a service or port to the public Internet due to operational requirements. In these cases, the PWS should use an MFA service (e.g., Duo, Okta, RSA) to restrict access to authorized users and a firewall to filter out unusual traffic, and the PWS should monitor network access and activity logs for unusual actions that may indicate a cyberattack.

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control AC-17 (page 48) and SC-7 (page 297) for more information on

"Remote Access" and "Boundary Protection". *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

DHS CISA Alert AA21-042A & AA21-287A: See these resources for information on various water system breaches from 2019-2021, including the one on Oldsmar Florida's water facility. *https://www.cisa.gov/uscert/ncas/alerts/aa21-042a*; *https://www.cisa.gov/uscert/ncas/alerts/aa21-287a*

DHS CISA Cyber Hygiene Services: See this resource for more information on DHS's free vulnerability scanning service. *https://www.cisa.gov/cyber-hygiene-services*

Shodan: See this resource to search for Internet-connected assets on the PWS's network. *https://www.shodan.io/*

Vulnerability Management: Limit OT Connections to Public Internet

COST: **$$$**$ IMPACT: **MEDIUM** COMPLEXITY: **MEDIUM**

5.5: Does the PWS eliminate connections between its OT assets and the Internet?

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

Why is this control important?

Developers did not design SCADA and OT systems with security in mind, PWSs do not patch or update them regularly, and directly connecting them to the Internet can present a major cybersecurity risk to PWS operations. Therefore, a critical aspect of PWS cybersecurity is to know which SCADA or OT assets the PWS has connected to the Internet and remove the Internet connection if possible.

While a PWS should always avoid connecting OT assets to the Internet, operational needs (e.g., remote site management) may sometimes require these connections. The PWS can reduce the cyber risk introduced by these connections through compensating controls like MFA, firewalls, and centralized logging.

Additional Guidance

- When identifying if a PWS has connected OT assets to the Internet, assess both standard connectivity (e.g., the SCADA network connected to the IT network or Internet modem) and other methods (e.g., wireless or cellular) for connecting OT assets to the Internet.
- A PWS should formally justify Internet connections to any OT assets and include compensating controls.

Implementation Tips

As mentioned in Factsheet 5.4, a PWS can search for Internet-exposed OT assets by using Shodan or DHS CISA's free vulnerability scanning services. An example of an easily overlooked connection between OT systems and the Internet is the use of cellular modems to connect remote assets (e.g., tanks, lift stations, wells) to the primary SCADA system. When used, cellular modems should be on the telecom provider's private networks whenever possible.

The PWS should create a process for justifying and documenting the operational need for an OT connection to the Internet with the OT cybersecurity lead. When operational needs require an approved OT connection to the Internet, the PWS should use the compensating controls detailed in Factsheet 5.4 to mitigate the cyber risk this connection creates.

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control AC-17 (page 48) and SC-7 (page 297) for more information on "Remote Access" and "Boundary Protection". *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

DHS CISA Cyber Hygiene Services: See this resource for more information on DHS' free vulnerability scanning service. *https://www.cisa.gov/cyber-hygiene-services*

Shodan: See this resource to search for Internet-connected assets on the PWS's network. *https://www.shodan.io/*

COST: **$**$$$ IMPACT: **HIGH** COMPLEXITY: **LOW**

6.1: Does the PWS include cybersecurity as an evaluation criterion for the procurement of OT and IT assets and services?

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

Why is this control important?

Granting a vendor access to a PWS network to perform a service (e.g., maintenance, configuration changes) or installing new hardware or software can add a new way for attackers to breach the network. In many circumstances, it is more convenient and cost-effective for a vendor to remotely access a network without being physically present at the PWS. However, if the vendor does not effectively secure its own computer systems, any malware or infections on the vendor's systems can migrate onto PWS systems.

Installed hardware or software may have unintentional weaknesses (i.e., vulnerabilities) that an attacker can use to enter a system. Further, an attacker (with or without the knowledge of the vendor) can intentionally insert vulnerabilities into hardware or software to introduce a weakness to the PWS network. The 2020 SolarWinds Attack is an example of such an attack that affected several Federal Government agencies.

Concerns that foreign governments could intentionally place weaknesses in hardware products exported from their country has led the Federal Communications Commission to ban certain vendors from U.S. Federal Government networks as well as from importation and sale in the U.S. Implementing this control will help the PWS to buy more secure products and services, reducing cyber risk.

Additional Guidance

- Given two offerings of roughly similar cost and function, the PWS should give preference to the more secure offering and/or supplier.
- When a PWS is looking to procure new IT or OT assets, insert cybersecurity requirements in the procurement process at the earliest stage so that vendors responding to the bid request will know to include these requirements up-front.

Implementation Tips

If a PWS gives a vendor remote access to a network, the PWS should require the vendor to use secure techniques such as a Virtual Private Network (VPN) and MFA. The PWS can also implement firewalls to filter out unusual traffic as well as monitor and log network activity. The Department of Energy resource below provides example procurement language for vendor cybersecurity requirements that PWSs can insert into vendor contracts.

To evaluate hardware and software vendors and reduce the cyber risk they present to PWS assets, PWS employees can ask vendors about their cybersecurity practices and research

them online to get a sense of their overall cyber safety. A PWS can use government advisories to research potential vendors, as well as search vulnerability databases (i.e., the Known Exploited Vulnerabilities (KEV) and National Vulnerability Database (NVD)) (See Factsheet 5.1).

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control SR-6 (page 369) and SR-5 (page 368) for more information on "Supplier Assessments and Reviews" and "Acquisition Strategies, Tools, and Methods". *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

GAO-22-104746 - Federal Response to SolarWinds and Microsoft Exchange Incidents: See the "What GAO Found" section for more information on the 2020 SolarWinds Supply Chain Attack. *https://www.gao.gov/products/gao-22-104746*

DHS CISA Known-Exploited Vulnerabilities (KEV): See this resource for vulnerabilities that attackers have already used. *https://www.cisa.gov/known-exploited-vulnerabilities-catalog*

NIST National Vulnerability Database (NVD): See this resource for a list of publicly known vulnerabilities. *https://nvd.nist.gov/vuln/search*

FCC – Enacted Vendor Hardware Bans: See these resources for details on current bans of vendor hardware.

https://www.fcc.gov/document/fcc-designates-huawei-and-zte-national-security-threats

https://www.fcc.gov/document/fcc-bans-authorizations-devices-pose-national-security-threat

Department of Energy (DOE) Cybersecurity Procurement Language: See this resource for example cybersecurity procurement language to include in vendor contracts. *https://www.energy.gov/ceser/articles/cybersecurity-procurement-language-energy-delivery-april-2014*

DHS CISA Alerts: See this resource to sign up for email alerts from DHS CISA's National Cyber Awareness System regarding new vulnerabilities. *https://www.cisa.gov/uscert/ncas/alerts*

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

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.

Why is this control important?

Factsheet 6.1 discusses the cyber risk that vendors can present to a PWS network. If a software or hardware vendor does not integrate security into the product design or is the victim of a cyberattack itself (e.g., the 2020 SolarWinds Attack), then the vendor may introduce weaknesses (i.e., vulnerabilities) into PWS computer systems. An attacker may then exploit those vulnerabilities at the PWS.

While many vendors proactively communicate information to customers, some vendors may hesitate or conceal discovery of security incidents or vulnerabilities in their products due to uncertainty or liability concerns. Receiving timely notification of vendor security incidents and vulnerabilities gives the PWS the opportunity to prevent or respond to potential attacks; therefore, PWSs should include a contractual notification requirement in procurement documents.

Additional Guidance

- When reviewing cybersecurity requirements within contracts, review both service provider contracts and hardware/software vendor agreements (e.g., OT integrator, IT vendor).

Implementation Tips

To ensure that other organizations honor their notification responsibilities, PWSs can include them in procurement contracts for hardware and software products and Service-Level Agreements (SLAs) for services. The PWS can choose a reasonable, risk-informed timeframe that it expects the vendor to notify the PWS of newly discovered vulnerabilities in a vendor's offerings and cyberattacks on the vendor's computer systems. The PWS can then include clauses requiring these notification timeframes in their future procurement contracts and SLAs with vendors as well as the penalties if the vendor does not meet these requirements.

The Department of Energy resource below provides example procurement language for vendor cybersecurity requirements that PWSs can insert into vendor contracts.

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control SR-8 (page 371) for more information on "Notification Agreements". *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

GAO-22-104746 - Federal Response to SolarWinds and Microsoft Exchange Incidents: See the "What GAO Found" section for more information on the 2020 SolarWinds Supply Chain Attack. *https://www.gao.gov/products/gao-22-104746*

Department of Energy (DOE) Cybersecurity Procurement Language: See section 3.3 on "Problem Reporting" within this resource for example cybersecurity language to include in vendor contracts. *https://www.energy.gov/ceser/articles/cybersecurity-procurement-language-energy-delivery-april-2014*

COST: **$**$$$ IMPACT: **HIGH** COMPLEXITY: **LOW**

7.1: Does the PWS 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)?

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.

Why is this control important?

Reporting incidents to outside agencies can help PWSs better respond to and recover from a cybersecurity incident. Reported information may also help stop the cybercrime from occurring at other PWSs and organizations. WaterISAC and local/state fusion centers also encourage reporting of cyber incidents and suspicious activity, as authorities can analyze the information to help provide trend information and awareness to the water sector.

Additional Guidance

- Develop a procedure and report template for reporting cybersecurity incidents promptly.
- Identify the PWS personnel responsible for reporting to external organizations.
- Specify escalation procedures (e.g., who the PWS notifies when and why) for reporting to the identified external organizations and the timeframes for reporting information. Flow diagrams or other visuals can help PWS personnel to understand in what order they should notify others and what information they should report.
- Distribute the reporting procedure and template to PWS personnel. Include this information in other emergency response documents, like the PWS emergency response plan or cybersecurity incident response plan.
- Under the Cyber Incident Reporting for Critical Infrastructure Act of 2022, the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) will establish procedures that may apply to PWSs. EPA will revise this guidance as necessary when CISA issues those procedures.
- If the PWS subscribes to cyber insurance or has a cyber incident response retainer, include these providers as contacts within the written procedure. There are often required reporting timeframes associated with making claims against cyber insurance or incident response retainers.

Implementation Tips

The written procedure should include the following:

- Contact information for reporting to the following:
  - The PWS's local law enforcement agency.

- DHS CISA – impacted organizations should submit an online CISA incident report, send an email to report@cisa.gov, or call 888-282-0870.
- The Federal Bureau of Investigation (FBI) – impacted organizations should contact their nearest FBI field office or submit a report through the Bureau's Internet Crime Complaint Center (IC3).
- The WaterISAC and local/state fusion centers – to report to WaterISAC, the PWS can submit an online WaterISAC report, email analyst@waterisac.org, or call 866-426-4722.
- The PWS's cyber insurance provider or cyber incident response retainer holder (if applicable).

The report template should include the following:

- Date and time when the PWS detected the incident
- Date and time when the incident occurred
- Brief description of incident including identification of potential attack method
- List of impacted assets
- Identification of any personally identifiable information (PII) that the incident may have compromised
- Date, time, and description of response/corrective actions that the PWS completed
- PWS personnel/vendor(s) involved in incident detection and response

Any information that the PWS shares with DHS or FBI, or any other federal government agency, is protected critical infrastructure information (PCII) and those agencies will not share it with the public. For more information, see CISA's PCII Fact Sheet.

Resources

Report to CISA: Provides information on how to report incidents and suspicious activity. *https://www.cisa.gov/report*

Report to the FBI: Provides information on how to report cybercrime reports. *https://www.fbi.gov/investigate/cyber*

Report to WaterISAC: Provides information on how to report incidents and suspicious activity. *https://www.waterisac.org/report-incident*

CISA's PCII Fact Sheet: Explains the protections offered by the PCII program. *https://www.cisa.gov/publication/pcii-fact-sheet*

COST: **$**$$$ IMPACT: **HIGH** COMPLEXITY: **LOW**

7.2: Does the PWS have a 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.

Why is this control important?

A PWS's IR plan describes the PWS's strategies, resources, and procedures to prepare for and respond to a cyber incident. The cybersecurity IR plan is essential in helping a PWS recover quickly from cybersecurity incidents. The PWS can incorporate the IR plan into their Emergency Response Plan (ERP).

Additional Guidance

- Identify personnel, OT and IT support staff, and vendors that the PWS should include in the development or update of the IR plan.
- Develop the cybersecurity IR plan to include the following:
  - Defined roles and responsibilities and actions that all PWS personnel will take during and after an incident.
  - Procedures to operate the PWS in manual mode, or alternate procedures to maintain water service if an attack compromises the OT system.
  - References to other relevant response plans and procedures as needed.
  - Diagrams and other visuals to help all PWS personnel understand their roles, responsibilities, and actions.
  - Template forms that PWS personnel can use to record decisions, actions, and expenditures.
  - Procedures and contact information for where to report the incident (see Factsheet 7.1)
- Distribute the IR plan and train all PWS personnel on the new cybersecurity procedures or steps in the IR plan. One method to train PWS personnel is conducting drills and exercises.
- Review the IR plan annually, at a minimum, and make changes as needed, such as changes in staff, vendors, and contact information.
- Update the IR plan after any significant changes to PWS OT and IT systems and based on any lessons learned from an exercise or actual incident.

Implementation Tips

A good starting place to develop an IR plan is EPA's "Incident Action Checklist for Cybersecurity". Conducting regular drills and exercises, such as tabletop exercises, is essential for an effective emergency response to minimize adverse impacts from a cyber incident. PWS should plan and conduct exercises with the participation of PWS staff, OT and IT support staff, vendors, and emergency response partners. If drills and exercises are new to the PWS, use a scenario that is simple and realistic. For example, develop a scenario that is based on a ransomware attack, since it is a common attack method. The goal is to exercise and evaluate existing plans, policies, and procedures and update them with any lessons learned. Conducting exercises will also help build the PWS's cyberattack response capabilities. After conducting the exercises, the PWS should hold an exercise debrief. The debrief provides an opportunity for exercise participants to provide feedback on what happened during the exercise and any obstacles/challenges encountered, and to identify any gaps in the PWS's plans, policies, and procedures that it needs to address.

Resources

EPA's Emergency Response Plan Template and Instructions: Provides a template and instructions document for PWSs. *https://www.epa.gov/waterutilityresponse/develop-or-update-emergency-response-plan*

EPA's Incident Action Checklist for Cybersecurity: Provides a rip-and-run style checklist to help PWSs prepare for, respond to, and recover from cyber incidents. *https://www.epa.gov/sites/default/files/2017-11/documents/171013-incidentactionchecklist-cybersecurity_form_508c.pdf*

WaterISAC's 15 Cybersecurity Fundamentals: Page 35 provides information and resources to develop an IR plan. *https://www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20%28WaterISAC%29.pdf*

CISA's Cyber Incident Response tools: Provides incident response training and playbooks. *https://www.cisa.gov/cyber-incident-response*

EPA's Tabletop Exercise Tool: Provides users with resources to plan, conduct, and evaluate tabletop exercises. *https://ttx.epa.gov/*

COST: **$$**$$ IMPACT: **HIGH** COMPLEXITY: **MEDIUM**

7.3: Does the PWS 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.

Why is this control important?

Backups are a critical element of a PWS's restoration and recovery activities in the event of a cyber incident, hardware malfunction (e.g., hard drive failure), or physical destruction of equipment (e.g., fire, flood). With ransomware being a key cyber threat to PWSs, where attackers aim to encrypt files and make them unusable, backups are one of the most important first lines of defense to avoid having to pay ransoms and quickly restore operations.

Additional Guidance

- Identify all operational, customer, employee, financial, and other data that a PWS may lose or that an attacker may corrupt during an incident, and that the PWS would need to restore post-incident to resume normal operations.
- The PWS should store backup media separately from the systems being backed up whenever possible. This method will not only protect the data in the event of a cyber incident, but also in the event of incidents such as a fire or flood. This method can be done by using off-site, cloud-based backups or manual backup rotations (e.g., having multiple backup drives and swapping them out periodically while the PWS stores one off-site).
- Establish a procedure to ensure that the PWS is following the backup process on the specified schedule and that file backups are useable. At a minimum, these actions should include spot-checking the file size and modification date of backup files on recovery media and/or validating that the PWS can individually recover the files.
- For OT assets, be sure that the backups include elements such as PLC logic and HMI graphics so that the PWS can quickly restore these items as well.
- At a minimum, the PWS should backup systems and test backups on an annual basis.

Implementation Tips

The PWS should perform backups using the "backup-in-depth" approach, with layers of backups (e.g., local, facility, disaster) that are time-sequenced such that recent local backups are available for immediate use and secure backups are available to recover from a large cybersecurity incident. The "backup-in-depth" approach relies upon a utility having three copies of their data, utilizing at least two different storage media, and storing at least one copy remotely offsite or in the cloud. The PWS should use multiple backup/restore

approaches and storage methods to ensure that backups are rigorously produced, securely stored, and appropriately accessible for restoration.

Resources

NIST Standard 800-82, Guide to Industrial Control System (ICS) Security: Additional information on redundancy and fault tolerance can be found in Section 5.13 (page 5-21). *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf*

NIST Standard 800-34, Contingency Planning Guide for Federal Information Systems: Additional information on general backup procedures and best practices can be found in Section 3.4.2 (page 21). *https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf*

COST: **$$**$$ IMPACT: **MEDIUM** COMPLEXITY: **MEDIUM**

7.4: Does the PWS 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.

Why is this control important?

A well-defined network topology helps System Administrators to locate faults, troubleshoot issues, and allocate network resources. Network diagrams/topologies are an important reference point to diagnose network issues and identify potential security vulnerabilities, as they represent both physical and logical layouts. A complete and up-to-date logical network diagram is essential to cyber disaster recovery.

Additional Guidance

- To create an accurate network topology, the PWS should conduct a network survey to validate any known and any previously unknown connection pathways. When conducting this survey, include not just traditional ethernet-based network connections, but also look for less traditional pathways such as serial, wireless, dial-up, and line-of-sight communications. Where remote assets (e.g., tanks, lift stations) are present, evaluate how these assets communicate with the PWS network.
- After the PWS completes the network survey, document the results and keep the results up to date. PWS networks may be quite complex and documented survey results will help ensure that the PWS does not overlook or forget communications channels over time. Survey documentation should include details about the specific assets on the network, any connections, and the method used for the connection (e.g., hard-wired, wireless). The PWS should especially focus on systems connecting directly to the public Internet and any communication pathways between the OT (e.g., SCADA) and IT (i.e., business enterprise) systems.

Implementation Tips

To be efficient, a PWS can perform a network survey at the same time as the review of asset configuration detailed in Factsheet 2.5 and the asset inventory process detailed in Factsheet 2.3. A free and easy-to-use website that can help to build network diagrams is Lucidchart. Microsoft provides a brief breakdown of what to include in a network diagram. CISA's CSET tool is a free version of basic Visio and OT-related graphics for building network topologies.

Consider including the network diagram in the PWS Cybersecurity Incident Response (IR) Plan, or Emergency Response Plan, as this information can be valuable for incident response.

Resources

Lucidchart: Lucidchart is a web-based diagramming application that allows users to visually collaborate on drawing, revising, and sharing charts and diagrams and improve processes, systems, and organizational structures.
https://www.lucidchart.com/pages/examples/diagram-maker

Microsoft - Create a Basic Network Diagram: If the PWS uses Microsoft Visio software, this page describes how the basic network diagram template includes standard shapes for servers, computers, and other parts of a PWS network.
https://support.microsoft.com/en-us/office/create-a-basic-network-diagram-f2020ce6-c20f-4342-84f7-bf4e7488843a

CISA CSET Tool: This stand-alone desktop application guides a PWS through a systematic process of evaluating its OT and IT assets including network diagramming.
https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr

COST: **$$$**$ IMPACT: **HIGH** COMPLEXITY: **HIGH**

8.1: Does the PWS 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.

Why is this control important?

As organizations were using OT networks long before the invention of the Internet, makers of OT systems did not design them to the same level of security as IT networks. As the Internet became popular, organizations typically kept OT networks separate from IT systems, leaving what is called an "airgap" between OT and IT networks. Over time, however, organizations realized they could find operational efficiencies and cost savings by connecting OT and IT systems and sharing data between them.

While the concept of an airgap is still a popular response to OT/IT connectivity security concerns, it is virtually impossible to maintain one even in the most secure facilities (e.g., Stuxnet, 2010). Therefore, most cyberattacks that target OT networks begin as attacks on a PWS's IT network.

Segmentation is a security practice that digitally divides a PWS's OT and IT computer networks with the goal of improving network performance and cybersecurity. This control is important because a PWS can limit the ability of an attacker to access OT control systems after compromising the IT network.

Additional Guidance

- Only allow connections to the OT network from the IT network via approved assets and other approved means.
- By default, deny all connections to the OT network from the IT network unless explicitly allowed (by IP address and port) for specific system functionality.

Implementation Tips

A useful framework for understanding where to segment the network is the Purdue Enterprise Reference Architecture (PERA), or Purdue Model for short. This model separates OT and IT networks into layers, helping to differentiate the types of assets at each level of a control system network. Levels 0 through 3 consist of OT assets, and Levels 4 and 5 refer to the IT enterprise network.

Network segmentation primarily occurs between the OT and IT networks at Levels 3 and 4, where a PWS can establish a "demilitarized zone" as a buffer between OT and IT networks using hardware and software tools to monitor, log, and filter traffic. The most common tool that a PWS can use for network segmentation is to install a firewall at the boundary of the

OT and IT networks, which can deny all connections between OT and IT systems by default. With a firewall, a PWS can control information flow between subnetworks or systems by traffic type, source, destination, and other options.

Resources

NIST 800-82 (Revision 2) Guide to Industrial Control System (ICS) Security: See section 5.1 (page 5-1) for more information on "Network Segmentation and Segregation." *https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final*

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control AC-4 (page 28) and SC-7 (page 297) for more information on "Information Flow Enforcement" and "Boundary Protection". *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

NSA "Stop Malicious Cyber Activity Against Connected OT" Advisory: This advisory lists steps that a PWS can take to evaluate risks against its OT system via IT system connection and implement changes with current resources to realistically monitor and detect malicious activity. *https://media.defense.gov/2021/Apr/29/2002630479/-1/-1/1/CSA_STOP-MCA-AGAINST-OT_UOO13672321.PDF*

MITRE ATT&CK - Stuxnet: See "Replication Through Removable Media" for more information on Stuxnet's spread. *https://attack.mitre.org/software/S0603/*

SANS Institute – The Purdue Model and Best Practices for Secure ICS Architectures: See this resource for more information on the Purdue Model and where Network Segmentation occurs in an OT network. *https://www.sans.org/blog/introduction-to-ics-security-part-2/*

DHS CISA – Understanding Firewalls for Home and Small Office Use: See this resource for more information on selecting and configuring a firewall. *https://www.cisa.gov/tips/st04-004*

COST: **$$$**$ IMPACT: **MEDIUM** COMPLEXITY: **HIGH**

8.2: Does the PWS keep a list of threats and attacker 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.

Why is this control important?

Cyberattacks require several steps to break into and move within a PWS computer system. Attackers frequently employ common steps or methods during a cyberattack, known as TTPs. If a PWS is aware of common TTPs, then they can monitor for these TTPs on the PWS network and detect an attack before it disrupts or damages operations.

PWS should monitor both external and internal components as part of their OT and IT cybersecurity program. External monitoring observes events at the boundary of the network, and internal monitoring captures events within PWS systems. This control is important because it helps a PWS be aware of and detect threats to their OT and IT networks.

Additional Guidance

- Adopt measures and mitigations recommended in CISA Alerts, such as firewall traffic filtering rules, suspicious network traffic alerting, or commercial prevention and detection systems to detect key threats where feasible.
- If a PWS identifies a validated threat within the IT or OT network, the PWS should follow its Incident Response plan (see Factsheet 7.2) for the containment, removal of, and recovery from the threat.

Implementation Tips

Alerts and advisories provide timely information about current cybersecurity issues and TTPs, vulnerabilities, and exploits. Register to receive alerts and advisories via email from DHS CISA. Other helpful sources for understanding TTPs and actions an attacker may take to move across an OT or IT network are the MITRE ATT&CK and MITRE ATT&CK for ICS frameworks, respectively.

There are many commercially available tools that a PWS can use to monitor for certain types of cyberattacks or intrusions into the PWS network. These tools include Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS), firewall rules that filter out and alert on certain traffic, and ICS network monitoring tools.

These tools can send alerts to a central monitoring system, often called a System Information and Event Monitoring (SIEM) tool. A SIEM tool pulls data from many sources

(e.g., IDS/IPS, firewalls, network monitoring tools, Windows Events) into one dashboard and can alert the PWS to unusual or malicious network activity.

Resources

NIST 800-82 (Revision 2) Guide to Industrial Control System (ICS) Security: See section 6.2.17 (page 6-38) for more information on "System and Information Integrity". *https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final*

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control SI-4 (page 336) for more information on "System Monitoring". *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

DHS CISA Alerts: See this resource to sign up for email alerts from DHS CISA's National Cyber Awareness System regarding new vulnerabilities. *https://www.cisa.gov/uscert/ncas/alerts*

MITRE ATT&CK and MITRE ATT&CK for ICS: See these resources for more information on common TTPs in OT and IT systems, respectively. *https://attack.mitre.org/matrices/ics/*; *https://attack.mitre.org/matrices/enterprise/*

COST: **$**$$$ IMPACT: **MEDIUM** COMPLEXITY: **LOW**

8.3: Does the PWS 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.

Why is this control important?

While attackers have many possible ways to enter a network, the most common and successful method is through email-related attacks such as phishing, spoofing, and interception. Phishing is an attack method where employees are sent an email with a malicious file, link, or request. If the employee opens it, a malicious file may load malware onto the PWS network, a malicious link may download malware or steal employee credentials, or a malicious request may trick an employee into providing credentials or PWS funds.

Spoofing is a method that attackers often use together with phishing, where an attacker designs malicious email to look like it came from an acceptable source. This deception can be done by copying the style and email address of a known company.

Interception is a method where an attacker can place themselves in between the sender and receiver of an email, giving them the opportunity to steal the email and its contents.

PWS employees should be aware of these attack methods, but there are also technical controls that can filter out some of these malicious emails before they get to employees. This control is important because using these technical controls can reduce the risk of email-based attacks to PWS operations.

Additional Guidance

- On all PWS email infrastructure, enable STARTTLS (Start Transport Layer Security), SPF (Sender Policy Framework), and DKIM (DomainKeys Identified Mail). Also enable DMARC (Domain-based Message Authentication, Reporting, and Conformance) and set to "reject." DHS CISA recommends these email security settings.

Implementation Tips

PWSs should conduct employee training and awareness campaigns to complement these recommended technical controls and reduce the overall risk of email-based attacks to the PWS network.

While the PWS should avoid all connections between OT and the public Internet, if possible (see Factsheet 5.5), the PWS should not set up any OT asset to receive email since email attacks are common and often effective.

Resources

DHS CISA BOD 18-01: See this resource for more information on how to configure various email security controls. *https://www.cisa.gov/binding-operational-directive-18-01*

NIST 800-82 (Revision 2) Guide to Industrial Control System (ICS) Security: See section 5.8.8 (page 5-18) for more information on "Simple Mail Transfer Protocol (SMTP)". *https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final*

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control SI-8 (page 348) and SC-18 (page 311) for more information on "Spam Protection" and managing macros, referred to as "Mobile Code". *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

APPENDIX C: Glossary of Terms

Term	Definition
Access Control Lists	Lists that identify those individuals that may access an Operational Technology (OT) and/or Information Technology (IT) system.
Active Services	Programs running in the background.
Asset	A cyber facility, device, information, or process that has value.
Automatic Account Lockout or Account Lockout Threshold	Policy that determines how many times a person can attempt to log in with incorrect credentials before the system locks them out.
Bastion Host	A special-purpose computer on an OT or IT network that a Public Water System (PWS) specifically designs and configures to withstand cyberattacks.
Backup	The process of creating a copy of critical PWS data that can be used for recovery in case the original data is lost or corrupted.
Compensating Controls	Security and privacy controls that a PWS implements in lieu of the baseline controls described in National Institute of Standards and Technology (NIST) Special Publication 800-53. Compensating controls provide equivalent or comparable protection for an OT or IT system.
Configuration	The setup of an OT or IT system or component, including the conditions, parameters, and specifications.
Control	A practice or measure that a PWS uses to prevent, detect, and mitigate cyber threats and attacks. Practices range from physical controls, such as removing USB ports in laptops, to technical controls, such as using firewalls and multi-factor authentication.
Control System	A system that assists in implementing a procedure or process (e.g., water treatment). Control systems include

Term	Definition
	Supervisory Control and Data Acquisition (SCADA), Distributed Control System (DCS), Programmable Logic Controllers (PLCs), and other types of industrial control systems.
Credentials	Information that is unique to a specific user and is required to log on to a system or a program. For example, a username and password.
Data Loss Prevention (DLP)	The practice of detecting and preventing data breaches, exfiltration (theft or unauthorized removal or movement of any data from a device), or unwanted destruction of sensitive data. Organizations use DLP to protect and secure their data and to comply with regulations.
Demilitarized Zone (DMZ)	A perimeter network that acts as a fence and governs the exchange of information between internal and external computer networks. It regulates how information flows from an internal network to an external network and who from the external network can access the internal network. It is often used between the OT and IT networks of a PWS.
Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA)	CISA leads the national effort to understand, manage, and reduce risk to the nation's cyber and physical infrastructure. CISA develops and publishes a variety of information, resources, tools, and training for the water sector and other critical infrastructure sectors.
Devices	Pieces of computer hardware that include desktops, laptops, servers, and tablets.
DomainKeys Identified Mail (DKIM)	Email authentication method to verify the authenticity of emails.
Domain-Based Message Authentication, Reporting, and Conformance (DMARC)	A protocol that uses Sender Policy Framework (SPF) and/or DKIM records to authenticate emails. It allows for the rejection of fraudulent emails.
Embedded Code	Code that a third-party website, such as YouTube or Twitter, generates that a user can copy and paste into

Term	Definition
	their own webpage. This embedded code will then show the same media, application, or feed on the user's web page as it does on the original website.
Emergency Response Plan (ERP)	A plan that describes strategies, resources, plans, and procedures PWSs can use to prepare for and respond to a natural or man-made incident that threatens life, property, or the environment.
Encrypt	Process by which a PWS converts plain text or data into coded or “ciphered” text/data.
Encryption	Any procedure that a PWS uses to convert plain text or data into coded or “ciphered” text/data to prevent anyone but the intended recipient from decoding and reading the text or data.
Executable	A piece of computer code or programming that can perform set tasks according to its encoded instructions. Executable files are used by a computer program or routine.
Fault Tolerance	The ability of a system (e.g., computer, OT or IT network, cloud cluster) to continue operating without interruption when one or more of its components fail.
Fast Identity Online (FIDO)/Client to Authenticator Protocol (CTAP)	Developed by the FIDO Alliance, the CTAP enables communication without the use of passwords between an external authenticator (e.g., mobile phones, connected devices) and another client (e.g., browser) or platform (e.g., operating system such as Microsoft Windows).
FBI Internet Crime Complaint Center (IC3)	A division of the Federal Bureau of Investigation focused on suspected Internet-facilitated criminal activity.
Firewall	A device that restricts data communication between two connected networks. A firewall may be either an application installed on a general-purpose computer or a separate device that allows or rejects information flow between networks. Typically, a PWS uses firewalls to

Term	Definition
	define zone borders, such as between OT and IT systems at a PWS.
Firmware	Software program or instructions programmed on the flash read-only memory (ROM) of a hardware device. It enables the device to communicate with other computer hardware.
Group Policy Object (GPO)	Allows a System Administrator to dictate how users and computers will interact. Group policies are primarily security tools and a PWS can use them to apply security settings to users and computers, such as requiring a minimum password length.
Human-Machine Interface (HMI)	User interface or dashboard that connects a user to a machine, system, or device. The term "HMI" is commonly used in the context of an industrial process, such as interacting with a SCADA system. For example, a PWS operator might use an HMI to check if a certain pump is operating.
Internet Protocol (IP) Address	A numerical address that identifies a devise on the Internet or local network.
Incident Response (IR) Plan	A set of predetermined and documented procedures to detect and respond to a cyber incident. Some PWSs may include their cybersecurity IR plan as part of their PWS Emergency Response Plan.
Information Sharing and Analysis Centers (ISACs)	An organization that collects, analyzes, and disseminates actionable threat information to its members and provides them with tools to mitigate risks and improve resiliency. For example, WaterISAC provides these services to PWSs.
Information System	Interconnected set of information resources under the same direct management control that share common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Term	Definition
Information Technology (IT)	A set of resources that an organization uses for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Industrial Control System (ICS)	A system used to control industrial processes such as water treatment and distribution. ICSs include SCADA systems (frequently used at PWSs to control geographically dispersed assets), distributed control systems, and smaller control systems using PLCs to control localized processes.
Interception	Interception allows attackers to access data, applications, or systems, and are primarily attacks against confidentiality. This could be unauthorized file viewing or copying, eavesdropping on phone conversations, or reading another person's email. These attacks can be conducted against data at rest (e.g., stored on a server) or in motion (e.g., an email in transit from sender to receiver).
International Electrotechnical Commission (IEC)	A global, not-for-profit membership organization that brings together 173 countries and coordinates the work of 20,000 experts globally. It facilitates electricity access, and verifies the safety, performance and interoperability of electric and electronic devices and systems, including consumer devices such as mobile phones, refrigerators, office and medical equipment, IT, electricity generation, and much more.
International Society of Automation (ISA)	A non-profit professional association founded in 1945 to create a better world through automation. ISA develops widely used global standards, certifies professionals, provides education and training, publishes books and technical articles, hosts conferences and exhibits, and provides networking and career development programs for its members and customers around the world.
International Society of Automation/International	The ISA/IEC 62443 series of standards, developed by the ISA99 committee and adopted by the IEC, provides a

Term	Definition
Electrotechnical Commission (ISA/IEC) 62443	flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs).
Intranet	A local communications network that is often used to improve communication, collaboration, and engagement within an organization. It typically excludes anyone from outside the organization.
Intrusion Detection System/Intrusion Protection System (IDS/IPS)	Both systems are placed within a network to alert when an unwanted intrusion has occurred. An IDS is designed to only provide an alert about a potential incident. An IPS, on the other hand, acts to block the attempted intrusion or otherwise remediate the attack.
Inventory	The formal listing or record of the organizational property at a PWS.
Jump Box	A hardened and monitored device that spans two dissimilar network security zones and provides a controlled means of access between them. It essentially serves as a gated bridge between the zones.
Known Exploitable Vulnerabilities (KEV) Catalog	A list of vulnerabilities that CISA has identified as being exploited or that threat actors have used to conduct attacks.
Least Privilege	The principle that an organization should design cybersecurity so that it grants each user the minimum system resources and authorizations needed to do their job.
Log	A record of the events occurring within a PWS's OT and IT systems and networks.
Media Access Control (MAC) Address	A unique identifier assigned to a network interface controller (NIC) for use as a network address. Device manufacturers typically assign MAC addresses, so devices come with this address already assigned to them,

Term	Definition
	unlike IP addresses. Also referred to as the hardware address or physical address.
Macro	A configured action that allows users to automate tasks and add functionality in files (e.g., a command button and an associated macro on a form). The macro contains the commands that the button will perform each time a user clicks it.
MITRE ATT&CK	A guideline for classifying and describing cyberattacks and intrusions.
Multi-factor Authentication (MFA)	A feature that requires more than one distinct authentication factor, such as a code texted to a cell phone, to activate a device or login into an account.
National Vulnerability Database (NVD)	The NVD was established to provide a U.S. government data repository about software vulnerabilities and configuration settings.
Network Segmentation	Dividing a network into multiple segments or "subnets," each acting as its own small network. This feature allows for control of the information flow between subnets. PWSs can use segmentation to improve monitoring, boost performance, localize technical issues, and enhance cybersecurity.
National Institute of Standards and Technology (NIST)	An organization that develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies, and the broader public.
NIST Cybersecurity Framework (CSF)	Voluntary guidance, based on existing standards, guidelines, and practices, for organizations such as PWSs to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, NIST designed the CSF to foster risk and cybersecurity management communications between internal and external organizational stakeholders.

Term	Definition
Network Switch	A device that connects users, applications, and equipment across a network so that they can communicate with one another and share resources.
Network Traffic	The amount of data that moves across a network during any given time.
Operating System (OS)	Software that serves as an interface between computer hardware and the user. Applications (e.g., Microsoft Office) require an environment to operate and perform tasks in. The OS helps users interact with applications and other hardware and programs. OS also performs tasks such as file, memory, and process management.
Operational Technology (OT)	The hardware, software, and firmware components of a system that a PWS uses to detect or cause changes in physical processes through the direct control and monitoring of physical devices. For many PWSs, this is a SCADA system.
Patches	Software and operating system updates that address security vulnerabilities within a program or product. Software vendors may choose to release updates to fix performance bugs and provide enhanced security features.
Personally Identifiable Information (PII)	Any information that permits the identity of an individual to be directly or indirectly inferred.
Protected Critical Infrastructure Information (PCII) Program	The PCII Program protects information not customarily in the public domain and related to the security of critical infrastructure or protected systems, including documents, records, or other information from federal, state, and local disclosure laws. This allows partners such as PWSs to securely share their critical infrastructure information with the DHS without fear of disclosure.
Phishing	Fraudulent emails, text messages, phone calls or websites that trick people into downloading malware, sharing sensitive information (e.g., Social Security and

Term	Definition
	credit card numbers, bank account numbers, login credentials), or taking other actions that expose themselves or their PWS to cybercrime.
Privileged Account	A user account that has more privileges than ordinary users. Privileged accounts might, for instance, be able to install or remove software, upgrade the operating system, or modify system or application configurations. These accounts might also have access to files that standard users are not able to access. At a PWS, a "System Administrator" would most likely have a privileged account.
Programmable Logic Controller (PLC)	A small industrial computer originally designed to perform the logic functions executed by electrical hardware (e.g., relays, switches, and mechanical timer/counters). PLCs have evolved into controllers with the capability of controlling complex processes, and PWSs frequently use them in SCADA systems.
Purdue Enterprise Reference Architecture (PERA), or Purdue Model	A six-layer model for ICS network segmentation that defines the system components found in each of the layers and the network boundary controls for securing each layer and ultimately the ICS network.
Remote Desktop Protocol (RDP)	A network communications protocol developed by Microsoft. It enables System Administrators to remotely diagnose problems that individual users encounter and gives users remote access to their physical work desktop computers. Support technicians often use RDP to diagnose and repair a user's system remotely.
Router	A device that communicates between the Internet and the devices at a PWS that connect to the Internet.
Server	A computer program or device that provides a service (such as sharing data or resources) to another computer program and its user, also known as the client.

Term	Definition
Supervisory Control and Data Acquisition (SCADA)	A type of industrial control system. It is a collection of both software and hardware components that allows users to control, monitor, and automate processes. SCADA systems help to gather and analyze real-time data.
Secure Sockets Layer (SSL)	A protocol that a PWS uses for protecting private information during transmission via the Internet.
Sender Policy Framework (SPF)	An email authentication method that helps protect outgoing email from being marked as spam by receiving organizations.
Service Level Agreement (SLA)	A commitment between a service provider (e.g., vendor) and a customer (e.g., PWS). Aspects of the service's quality and availability, as well as the parties' individual responsibilities, are agreed upon in advance.
Spoofing	A type of scam in which an attacker disguises an email address, display name, phone number, text message, or website URL to convince a target that they are interacting with a known, trusted source.
Start Transport Layer Security (STARTTLS)	A protocol used to ensure email is securely transported from one server to another.
Supply Chain Attack	A type of cyberattack that targets a trusted third-party vendor who offers services or software vital to the supply chain. Supply chain attacks are difficult to detect, as they rely on software that has already been trusted and can be widely distributed (e.g., SolarWinds attack).
System Administrator	Person responsible for managing, updating, and operating the computer system(s). This person can be an individual at the PWS or a vendor.
Security Information and Event Management (SIEM)	A tool that collects event log data from a range of sources (e.g., devices, software), identifies activity that deviates from "normal" with real-time analysis, and takes appropriate action. It helps organizations detect, analyze,

Term	Definition
	and respond to security threats before they interrupt operations.
Table-Top Exercise (TTX)	A discussion-based exercise where personnel with roles and responsibilities in a particular IR plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during a cyber emergency and their responses to a particular cyber incident. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.
Tactics, Techniques, and Procedures (TTPs)	This is the term used by cybersecurity professionals to describe the behaviors, processes, actions, and strategies used by an attacker to engage in cyberattacks.
Transparent Data Encryption (TDE)	TDE enables the user to encrypt sensitive data that is stored in databases at the file level. It protects data at "rest", not data in "transit."
Transport Layer Security (TLS)	An authentication and encryption protocol widely implemented in browsers and Web servers. Hyper Text Transfer Protocol (HTTP) traffic (a standard method for communication between clients and Web servers) transmitted using TLS is known as Hyper Text Transfer Protocol Secure (HTTPS).
Virtual Private Network (VPN)	A service that extends a private network across a public network (e.g., Internet) and provides a secure, encrypted channel between the user's device and the private network. A VPN allows users to conduct work remotely.
Vulnerability	A flaw or weakness in a piece of software or firmware that an attacker can use to modify application code, damage an asset, gain access to a network, or execute other malicious activity.
Wireless Access Point	A device that creates a wireless local area network, or WLAN, usually in an office or large building. An access

Term	Definition
	point connects to a wired router, switch, or hub and projects a WiFi signal within a designated area.