



Data Gathering

Begin the assessment by gathering information about the organization, industrial process, existing security controls, network architecture, policies and standards, and the organization's information attack space and threat landscape.

- **Company OSINT**—Conduct an open-source intelligence (OSINT) exercise. This involves gathering publicly available information using tools such as Google, Shodan, LinkedIn, etc. to learn what adversaries likely already know about your organization, operations, and Internet-connected devices. It is important to at least be aware of what information is publicly available, and then work to reduce it moving forward.
- **Policies, Procedures, Security Controls**—If security controls and governance were leveraged from IT, review and ensure that what is being produced or in place has been adapted to suit ICS-specific needs across ICS security controls, processes, and procedures in order to prioritize availability and the safety of engineering assets and operations.
- **Network and Traffic Flow Diagrams**—Review and verify that network architecture represents “as built” documentation with production network traffic, core network devices, services, and expected protocols. Services and protocols that are not required should be disabled through the hardening process to reduce attack surfaces.
- **Asset Inventory**—Generate discussions around which assets and applications are deemed critical to the process. If asset inventories are updated regularly – usually in a database with details on the hardware and software installed in the control network – they can be used with threat intelligence to drive proactive defensive operational changes and threat hunting.



Physical Walk-Through

The assessment team needs to understand the physical process that is being assessed.

- **Safety Training**—Most industrial sites require all personnel to complete safety training and wear personal protective equipment (PPE) before entering a site. Plan time for these tasks prior to arriving at a site.
- **Physical Security**—Physical security breaches can lead to cyber incidents. Document the scope of physical security and understand the related security controls deployed. Start with the front gate: observe authentication processes, tailgating opportunities, unlocked gates, doors propped open, fences with gaps, etc.
- **Process Walk-Through with Teams**—Physically walk through the site to understand the industrial process. Include process control engineers, network and security architects, field technicians, programmers, operators, managers, and facility owners. Start a discussion around what an impactful control system event would look like and how it could occur. Leverage the physical safety culture by drawing parallels between physical safety and ICS cybersecurity case studies.
- **Asset Inventory Updates**—Carefully inspect control and network cabinets to understand what technologies, hardware, and applications are deployed. Basic attributes to record include the site name, location, facility type, asset type and tag, description of asset function, impact on operations if unavailable, IP and MAC address, ICS protocols in use, model/manufacture, serial number, firmware version, and applications installed and their versions. Merge and verify newly captured information with existing inventories in a scalable, searchable, and secured database.



Active Defense Capabilities

Regular review of security events involving key assets can aid cyber investigations and engineering root cause analysis, and enable proactive threat hunting capabilities. Review security event log and monitoring capabilities by starting with the network, followed by critical endpoints and then field devices. Follow up by reviewing how logs are consolidated, correlated, and tuned by human defenders within Security Information and Event Management (SIEM). Use the following points to generate discussion:

- **Network Security Monitoring**—Monitoring of the network can be accomplished via a TAP or SPAN. A SPAN may be configured with existing technology if supported. The installation of a TAP may require a network outage. Full or partial (5-tuple) packet captures will be options for network collection. Understand which method of traffic collection is deployed or possible in the environment.
- **Servers, End Points**—Whitelisting anti-malware solutions can be more effective than traditional IT signature or heuristics-based solutions. Critical assets to review first include but are not limited to Data Historians, Human Machine Interface (HMI), Active Directory Domain Controller, and Engineering Workstations.
- **Field Devices**—Field devices such as Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), and other critical engineering assets may not have logging enabled by default. Review field device logging capabilities. Forward security event and device change logs to a SIEM for central management and event correlation. In some cases, older field device firmware can be updated to expand or enable logging capabilities.
- **Repeatable Process**—Effective active defense requires dedicated human defenders trained in ICS security and the control environment – regularly reviewing critical network events and system logs for suspicious activity.



Network Defense

Verify whether the Purdue Enterprise Reference Architecture Model is being followed. The Purdue Model suggests how to segment devices and systems within the control network based on levels. Each level can help establish a security enforcement boundary for separation and protection. These levels create natural points in a network to enable logging, network security monitoring, and enforcement of access control, and to assist with containment in incident response.

- **Level 5**—Internet, Cloud Services
- **Level 4**—Enterprise IT Business Systems
- **Level 3**—ICS Plant Site-Wide SCADA Controls
- **Level 2**—Local Supervisory, HMI, Engineering Workstations
- **Level 1**—Process Control, Field Devices
- **Level 0**—Sensors, Hardware Actuators

The following should be considered when assessing the security of each Level.

- **Network Boundaries**—Start with corporate network firewalls, control network firewalls, and demilitarized zones to ensure proper organization of assets at each level. Lower levels will have fewer network restrictions due to process requirements, yet should still be hardened. Only required services, ports, and protocols used for operations should be enabled.
- **Wireless Networks**—Cellular, Wi-Fi, Bluetooth, and other proprietary wireless connectivity can be used for critical communication channels between remote sites to acquire telemetry data and to send and receive control commands. Sweep for wireless networks beyond just Wi-Fi and verify network boundaries and access controls.



Security Configuration

Risk is significantly reduced by implementing a few basic access control concepts. Focus assessment efforts here first, and include physical security and related physical access systems.

- **Windows Active Directory**—The ICS Active Directory (AD) should not have trusted relationships or trusted forests with the corporate IT AD. Corporate AD and ICS AD credentials should be different. Review Windows Group Policy configurations to understand how security controls are implemented across Windows servers and workstations in ICS.
- **Network, Application, File Shares**—Review core network and system access, including core network appliances, field devices, web applications, HMIs, Data Historian applications, etc. Default vendor credentials should have been changed prior to go-live, authentication should be used where feasible, and logging should be enabled. Networked devices should be hardened. Review networked file shares to understand what types of sensitive information is stored on them and how it is accessed and protected. File shares and services not strictly required should be disabled to reduce attack surfaces.
- **Remote Access**—Review remote connectivity technologies, remote user accounts, and processes used by employees, vendors/integrators, and managed service providers. Ensure proper access control following the principle of least privilege, and ensure that multi-factor authentication and secure channels are in place. The use of a jump host for remote access is a common security concept to allow for controlled ingress/egress, monitoring of remote connections, and logging.

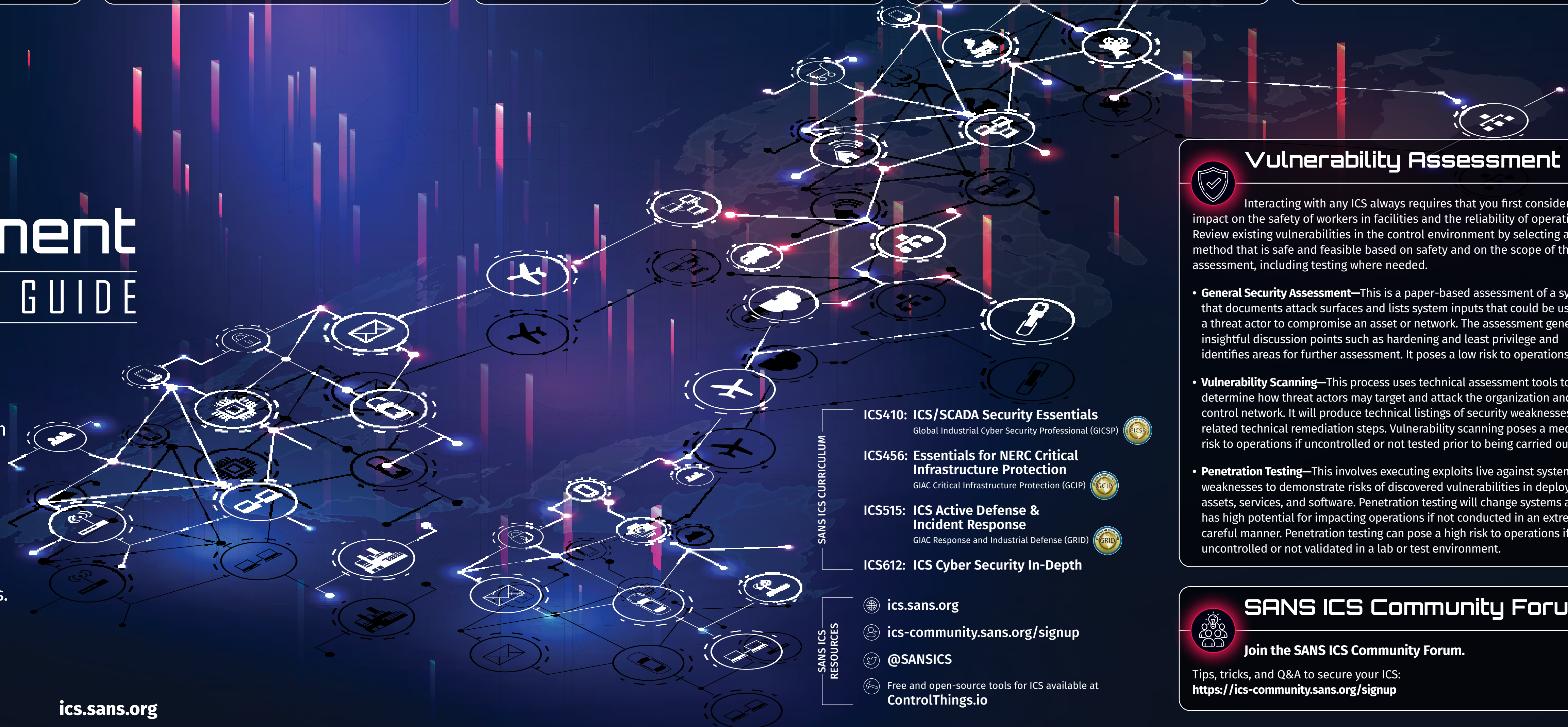
ICS Assessment Quick-Start Guide

This ICS Assessment Quick Start Guide provides a basic starting point for industrial control system (ICS) assessments that can be applied to all ICS sectors. Concentrating on several primary risk areas, this content aims to help organizations identify opportunities to improve newly established ICS security programs.

SANS The most trusted source for cybersecurity training, certifications, degrees, and research

ICSPS_v11_06-21
This poster was created by Dean C. Parsons. ©2021 Dean C. Parsons. All Rights Reserved.

ics.sans.org



Vulnerability Assessment

Interacting with any ICS always requires that you first consider the impact on the safety of workers in facilities and the reliability of operations. Review existing vulnerabilities in the control environment by selecting a method that is safe and feasible based on safety and on the scope of the assessment, including testing where needed.

- **General Security Assessment**—This is a paper-based assessment of a system that documents attack surfaces and lists system inputs that could be used by a threat actor to compromise an asset or network. The assessment generates insightful discussion points such as hardening and least privilege and identifies areas for further assessment. It poses a low risk to operations.
- **Vulnerability Scanning**—This process uses technical assessment tools to determine how threat actors may target and attack the organization and control network. It will produce technical listings of security weaknesses and related technical remediation steps. Vulnerability scanning poses a medium risk to operations if uncontrolled or not tested prior to being carried out.
- **Penetration Testing**—This involves executing exploits live against system weaknesses to demonstrate risks of discovered vulnerabilities in deployed assets, services, and software. Penetration testing will change systems and has high potential for impacting operations if not conducted in an extremely careful manner. Penetration testing can pose a high risk to operations if uncontrolled or not validated in a lab or test environment.



SANS ICS Community Forum

Join the SANS ICS Community Forum.

Tips, tricks, and Q&A to secure your ICS:
<https://ics-community.sans.org/signup>

ICS410: ICS/SCADA Security Essentials

Global Industrial Cyber Security Professional (GICSP)



ICS456: Essentials for NERC Critical Infrastructure Protection

GIAC Critical Infrastructure Protection (GCIP)



ICS515: ICS Active Defense & Incident Response

GIAC Response and Industrial Defense (GRID)



ICS612: ICS Cyber Security In-Depth

ics.sans.org

ics-community.sans.org/signup

@SANSICS

Free and open-source tools for ICS available at ControlThings.io

ICS Security Program Maturity

This guide covers the basics of using the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) in order to understand the maturity of a security program implemented to protect control environments from any industrial control sector. www.nist.gov/cyberframework

Initiating an ICS Security Program



This process concentrates on seven NIST CSF function categories to help leadership, engineers, and administrators gauge the maturity of the current program and prioritize risk reduction. Tracking a metric for maturity in each area will help guide your efforts and increase engagement as you work to increase the maturity of your program.

- ID Identify
- PR Protect
- DE Detect
- RS Respond



Maturing an ICS Security Program

PR Incident Response Table Top Scenarios

Teams can walk through, discuss, create, and/or simulate the sample IR tabletop scenarios listed below to validate existing controls and help prepare for an incident. There are no wrong answers. The gaps identified should be documented and addressed.

Example IR Table Top Scenarios:

- **Ransomware**—An operator logs into the asset management server and sees a ransomware note on the desktop background and discovers that all project files appear to be encrypted.
- **Maintenance or Compromise**—An administrator account is observed logging into all Windows servers and workstations across the control network.
- **Strange HMI Activity**—Operators notice the mouse cursor moving and clicking on different portions of the HMI that are not consistent with normal operations.
- **Living off the Industrial Control Security Land**—Operators troubleshooting network issues notice excessive ICS protocol traffic (OPC, IEC104, Modbus/TCP) from several systems.
- **Unauthorized Physical Access**—The physical security team notices forced entry into a building. The team investigates and determines that several control cabinets were opened and closed.

PR Access Control

Control networks have unique requirements for management by company personnel and third-party partners.

- **Control Network Credentials**—These credentials should be unique to the control environment. The control network Active Directory (AD) should not have a trust relationship, nor should it synchronize with corporate domains.
- **Multi-Factor Authentication**—Like Windows AD, MFA should not be shared with the corporate environment and should be required, at a minimum, for all remote access.
- **Vendors and Integrators**—Third-party accounts should be restricted to specific roles, responsibilities, and assets. MFA should be required. A jump server should be used to avoid direct connections from the Internet to control system servers.
- **Managed Service Providers (MSPs)**—Many organizations share MSP services between the corporate and control networks. MFA should be required. A jump server should be used to avoid direct connections to control system servers from outside the control network.
- **Service Accounts**—Service accounts are used for many applications and should not share credentials between the corporate and control networks.

CRITICAL NOTE: Monitoring the use of credentials and MFA is the most important step to ensure that access control is an effective security control.

DE Logging and Monitoring

Logging and monitoring within the control network is most effective when prioritized to collect network events first and then system events. Collected data should then be consolidated, correlated, and evaluated for events that provide actionable intelligence. The following are prioritized starting points for this discussion:

- **Network Events**
 - IP Flow Information Export (IPFIX)
 - Network Boundary Activity
 - Network Device Monitoring Configurations (Span port and physical taps)
 - Network Security Monitoring
- **System Events**
 - Windows Active Directory Events
 - DNS Events
 - Windows Event Logs
 - Syslog Events (*nix systems, PLCs, Field Devices)
- **Managed Logging and Monitoring**
 - Central Logging Windows
 - Central Logging Syslog
 - Security Operations Center Monitoring and Alerting

RS Incident Response

Incident response (IR) plans and procedures specific to operational technology (OT) are necessary to help organize and guide IT, ICS, InfoSec, and OT teams to success during these stressful events.

It is important to assess currently documented procedures to investigate suspicious activity, respond to a compromise, and support the recovery process. Understanding your organization's level of IR maturity requires a review of the preparation measures already in place.

- **Roles and Responsibilities**—Who is in charge and which team members are responsible for IT, InfoSec, and OT actions?
- **Key Team Member Contact List**—Is an up-to-date call list maintained and does it include multiple contact methods and identify secondary points of contact?
- **War Room/Conference Line**—Is there a standard location and/or conference call setup for organizing the response team?
- **Vendor/Integrator/MSP Assistance**—Are there agreements with these parties to assist with the response efforts?
- **Third-Party Assistance**—Have teams (e.g., forensics, OT IR experts) that provide staff augmentation during IR events been identified, and are agreements in place?
- **Jump Bag**—Is the set of systems and tools (hardware, software, storage) necessary to interact with the different technologies in the control network in place?
- **IR Triage Team**—Is there a dedicated team familiar with the control network and the tools and training needed to conduct information gathering and forensic analysis, and to provide actionable intelligence to the IR team?
- **Table Top Scenarios (TTX)**—Have IR scenarios that include IT/InfoSec/OT/Physical Security team members been run to train individuals on their roles and responsibilities and identify gaps in IR procedures?

CRITICAL NOTE: Due to plant and public safety requirements, compromised control networks may stay operational for weeks or months. During this time, IR efforts will continue in a contained and controlled state with increased monitoring and vigilant control. Full eradication may occur only during the next scheduled plant maintenance window or similar event.

PR Network Segmentation and Isolation

- **Network Boundaries**—Network segmentation and isolation begin with network boundaries between the corporate network and the control network.
- **Remote Access**—Make remote access secure and available for operators, engineers, integrators, vendors, managed service providers (MSP), and others crossing these boundaries.
- **Internet Access**—There is always a path to the Internet, so it is critical to understand and periodically review and assess this path.
- **Cloud Access**—Vendors and integrators are increasingly leveraging cloud access for maintenance and management, so systems communicating with the cloud should be isolated from other control systems wherever possible.

ID Asset Inventory Management

Asset inventory management is one of the most important and challenging categories for all organizations. Asset identification can be accomplished using four methodologies: Physical Inspection, Passive Monitoring, Active Monitoring, and Configuration Analysis. Device categories include (but are not limited to):

- Control Hardware (PLCs, Field Devices)
- Network Devices
- Servers and Workstations
- Process Control Software
- Other Software
- Other IT and Internet of Things Devices
- Transient Systems and Devices
- Removable Media Devices

ID Policies

Standards, guidelines, and procedures built from corporate policies are not implementable within the control network without careful analysis of a number of considerations. The NIST Special Publication 800-82 Revision 2 Guide to Industrial Control Systems (ICS) Security outlines many of these considerations.

Organizations can develop control network policies by starting with and adapting current corporate policies. Customizing policies to account for the unique requirements of control environments will help the team understand the organization's business and operation requirements and allow it to build sound standards, guidelines, and procedures to ensure the availability, resiliency, and safety of the process.

Providing guidance for each of the NIST CSF functions and categories is a good beginning. The control network team can use this guidance to identify the standards, guidelines, and procedures it should develop for each area. The team can leverage the NIST 800-82 Revision 2 publication to guide its conversation and development.

PR Security Awareness

Corporate security awareness programs traditionally focus on users accessing corporate assets or services such as email, financial systems, and the Internet. Industrial control system security awareness programs focus primarily on the safety of people, the system, and physical security.

To strengthen the resilience and availability of safety and processes, it is important for workers, operating in both OT and IT environments, to complete basic training and review content from both OT and IT security awareness training programs.

Furthermore, IT, InfoSec, OT, and physical security personnel who have control network responsibilities should receive training on control network policies and on their individual responsibilities. That training should also teach them how to identify suspicious activity and encourage them to report the activity as a part of their normal response and recovery steps.