Sept. 23, 2026

Considerations for Critical Infrastructure Operators Working With Third-Party ICS Integrators

Introduction

The Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA)—hereafter referred to as the "authoring agencies"—have published this fact sheet to highlight considerations for critical infrastructure entities to reduce risk and minimize vulnerabilities when working with third-party industrial control system (ICS) integrators.

ICS is an umbrella term referring to integrated networks of hardware and software designed to monitor and automate physical processes, encompassing specialized control systems and devices, such as supervisory control and data acquisition (SCADA) systems and programmable logic controllers. Third-party integrators provide varying types of services for ICS, such as control system design, installation, operational data analysis, device support and service, and daily operational control.

Critical infrastructure owners and operators should maintain caution when granting third-party ICS integrators high levels of access or control over industrial processes, ensuring the principle of least privilege (PoLP), is applied. PoLP within OT environments lends itself to granting users, processes, and systems only the minimum access necessary to perform their assigned tasks, and no more. PoLP is designed to protect owners and operators. Not adopting principles such as PoLP could expose owners and operators to malicious cyber actors seeking to compromise critical infrastructure, possibly providing sensitive access to pathways that actors can exploit to cause disruptive and destructive effects to equipment and critical functions.

Critical infrastructure owners and operators should action the recommendations in this fact sheet to work with integrators to ensure secure practices and frameworks are put in place to reduce the risk of malicious actors exploiting third-party accesses to compromise critical infrastructure operational environments.

Examples of Risk and Exploitation

Much like IT systems, using third-party ICS integrators in critical infrastructure may inadvertently introduce security issues to a customer environment by exposing systems and services not pre-configured to the customer's security requirements. Critical infrastructure owners and operators that rely on third-party

integrators for system design face supply chain risks if integrators and owners and operators do not collectively enforce clear requirements for the secure procurement and handling of system components. Furthermore, third-party integrators that operate and host data outside of the United States may pose additional risks, as they may be subject to different data storage and management laws that do not meet the security needs of U.S. critical infrastructure entities.

According to FBI technical analysis, between March and April 2025, malicious foreign cyber actors gained access to the network of a U.S. industrial automation solutions company that offered services—such as system integration, engineering consulting, and SCADA programming—for industrial customers, including power utilities and transportation entities. While on the network, threat actors searched terms, including "customers" and "SCADA," and created nine `.zip` files consisting of approximately 800 files for presumed exfiltration, including customer SCADA information, ICS device details, and other schematics. Malicious cyber actors could leverage the exfiltrated information to later conduct disruptive attacks against operational environments and disrupt critical services.

Recommendations to Assess Risk

Critical infrastructure owners and operators should make risk-informed decisions when considering introducing third-party integrators into their networks and operations, guided by a robust understanding of the organizational risks posed by providing sensitive access to their systems.

Organizations should routinely conduct risk assessments to evaluate contracts that involve access to industrial systems, to determine impacts to the organization's data autonomy and process controls. Risk assessments should address hardware and software supply chain vulnerabilities introduced by integrator equipment, as well as the IT and OT security of these devices and their associated networks. When considering implementing foreign-owned integrators, critical infrastructure owners and operators should also include geopolitical considerations in their risk assessments, such as how the critical infrastructure entity may be directly or indirectly targeted based on the geopolitical climate.

Critical infrastructure owners and operators should consider the following questions in their risk assessments to safeguard the security of their operational systems when working with third-party ICS integrators:

What organizational data does the integrator store or have access to?

Critical infrastructure network designs, device specifications, logs, and other data can all be useful information for malicious cyber actors. When evaluating the risk of enabling integrators to store or access this data, consider the potential for a malicious cyber actor to access this data through the integrator's network.

Where is the data stored?

If the integrator is foreign-owned, consider whether the utility data is stored within the United States or internationally. If data is stored internationally, the laws of that respective country may govern it and may apply even if the integrator is a U.S. subsidiary.

Does the integrator have remote access for operational support?

If the integrator has remote access to the organization's ICS network, then there is a potential risk that a malicious cyber actor could gain access to the integrator's network and pivot into the utility's network to gain control of their systems. Consider the security of the organization's remote connections when evaluating the risk these potential access points pose to the organization's network.

Can the organization operate independently if the integrator is compromised?

Having redundancies in place and the ability to recover the system and operate without the integrator, especially for operationally critical processes, can reduce risk in the event of integrator compromise. Operators should maintain secure, offline backups of all software required to operate equipment to facilitate system recovery.

Recommendations to Reduce Risk

The authoring agencies recommend critical infrastructure owners and operators implement the following steps to reduce the risks associated with using third-party ICS integrators:

- **Include cybersecurity and supply chain cybersecurity in contracts and service agreements.** When preparing service agreements, include requirements on areas such as:
  - Data storage locations, information protection agreements, and protection of ICS data and design documentation,
  - Remote access capabilities,
  - Basics of the integrator's cybersecurity program,
  - Change management and patch management policies,
  - Actions taken to secure deployed components (e.g., changing default passwords, disabling unused ports),
  - Listing authorized personnel with access to systems, and
  - Processes that enable local engineering support when necessary, limiting required integrator intervention.
- **Evaluate devices with external internet exposure.** Organizations should work with integrators to understand where devices are hosted and minimize exposure by disconnecting devices from the public-facing internet.
- **Monitor and log remote access.** Ensure integrators access equipment using routes you are able to monitor. Use on-demand remote access if possible, so operators have to proactively allow remote access.
- **Request an inventory of all software and hardware supplied by the integrator**, as well as documentation for how it connects to your infrastructure and how it will be updated.
- **Practice procedures and maintain capabilities for manual operations**, keeping in mind, and accounting for, where third parties fit into the environment and recovery procedures.

Resources

- For guidance on asset inventories, see CISA's Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators.
- For additional information on SBOMs, see CISA's 2026 Minimum Elements for a Software Bill of Materials (SBOM).
- For guidance on supply chain risk management, see the Communications Sector Coordinating Council (CSCC) and IT Sector Coordinating Council's (SCC) Supplier, Products, and Services Threat Evaluation (to include Artificial Intelligence Risks and Mitigations), and NIST's Cybersecurity Supply Chain Risk Management.
- For additional information and resources concerning cyber threats to ICS, visit Industrial Control Systems for Cybersecurity Advisories and other cybersecurity guidance and best practices.

Contact Information

The authoring agencies strongly urge critical infrastructure operators to report suspicious cyber activity to the following entities:

- Report cyber activity to your local FBI field office or IC3, or contact CISA via CISA's 24/7 Operations Center at contact@cisa.dhs.gov or 1-844-Say-CISA (1-844-729-2472).
- Report any leads, threats, and suspected criminal activity by submitting an electronic tip, calling 1-800-CALL-FBI (1-800-225-5324), or contacting your local FBI field office.
  Note: This website cannot be used to report emergencies or immediate threat to life. For emergencies or immediate threat to life, please call 911.
- If you are a law enforcement entity, use the unclassified information-sharing system eGuardian (accessible via the Law Enforcement Enterprise Portal) for reporting suspicious activity reports to the FBI. **Note:** If the information is urgent, then contact your local FBI field office directly and follow up with an eGuardian report.

Disclaimer

CISA and the authoring agencies do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA and the authoring agencies.

Version History

September 23, 2026: Initial version.