JOINT
CYBERSECURITY
ADVISORY

TLP:CLEAR

Co-Authored by:

Product ID: AA25-212A

July 31, 2025

CISA and USCG Identify Areas for Cyber Hygiene Improvement After Conducting Proactive Threat Hunt at US Critical Infrastructure Organization

Summary

The Cybersecurity and Infrastructure Security Agency (CISA) and U.S. Coast Guard (USCG) are issuing this Cybersecurity Advisory to present findings from a recent CISA and USCG hunt engagement. The purpose of this advisory is to highlight identified cybersecurity issues, thereby informing security defenders in other organizations of potential similar issues and encouraging them to take proactive measures to enhance their cybersecurity posture. This advisory has been coordinated with the organization involved in the hunt engagement.

CISA led a proactive hunt engagement at a U.S. critical infrastructure organization with the support of USCG analysts. During hunts, CISA proactively searches for evidence of malicious activity or malicious cyber actor presence on customer networks. The organization invited CISA to conduct a proactive hunt to determine if an actor had been present in the organization's environment. (**Note:** Henceforth, unless otherwise defined, "CISA" is used in this advisory to refer to the hunt team as an umbrella for both CISA and USCG analysts).

During this engagement, CISA did not identify evidence of malicious cyber activity or actor presence on the organization's network, but did identify cybersecurity risks, including:

- Insufficient logging;
- Insecurely stored credentials;
- Shared local administrator (admin) credentials across many workstations;
- Unrestricted remote access for local admin accounts;
- Insufficient network segmentation configuration between IT and operational technology (OT) assets; and
- Several device misconfigurations.

In coordination with the organization where the hunt was conducted, CISA and USCG are sharing cybersecurity risk findings and associated mitigations to assist other critical infrastructure organizations with improving their cybersecurity posture. Recommendations are listed for each of CISA's findings, as well as general practices to strengthen cybersecurity for OT environments. These mitigations align with CISA and the National Institute for Standards and Technology's (NIST) Cross-Sector Cybersecurity Performance Goals (CPGs), and with mitigations provided in the USCG Cyber Command's (CGCYBER) 2024 Cyber Trends and Insights in the Marine Environment (CTIME) Report.

Although no malicious activity was identified during this engagement, critical infrastructure organizations are advised to review and implement the mitigations listed in this advisory to prevent potential compromises and better protect our national infrastructure. These mitigations include the following (listed in order of importance):

- **Do not store passwords or credentials in plaintext**. Instead, **use secure password and credential management solutions** such as encrypted password vaults, managed service accounts, or built-in secure features of deployment tools.
  - **Ensure that all credentials are encrypted** both at rest and in transit. Implement **strict access controls and regular audits** to securely manage scripts or tools accessing credentials.
  - Use code reviews and automated scanning tools to **detect and eliminate any instances of plaintext credentials on hosts or workstations**.
  - **Enforce the principle of least privilege**, only granting users and processes the access necessary to perform their functions.
- **Avoid sharing local administrator account credentials**. Instead, **provision unique, complex passwords for each account** using tools like Microsoft's Local Administrator Password Solution (LAPS) that automate password management and rotation.
- Enforce **multifactor authentication (MFA) for all administrative access**, including local and domain accounts, and for remote access methods such as Remote Desktop Protocol (RDP) and virtual private network (VPN) connections.
- Implement and enforce strict policies to only **use hardened bastion hosts isolated from IT networks equipped with phishing-resistant MFA to access industrial control systems (ICS)/OT networks**, and ensure regular workstations (i.e., workstations used for accessing IT networks and applications) cannot be used to access ICS/OT networks.
- **Implement comprehensive (i.e., large coverage) and detailed logging across all systems**, including workstations, servers, network devices, and security appliances.
  - Ensure logs **capture information such as authentication attempts, command-line executions with arguments, and network connections**.
  - **Retain logs for an appropriate period to enable thorough historical analysis** (adhering to organizational policies and compliance requirements) and **aggregate logs in an out-of-band, centralized location**, such as a security information event management (SIEM) tool, to protect them from tampering and facilitate efficient analysis.

For more detailed mitigations addressing the identified cybersecurity risks, see the **Mitigations** section of this advisory.

Table of Contents

Technical Details

Note: This advisory uses the MITRE ATT&CK® Matrix for Enterprise framework, version 17. See **Appendix: MITRE ATT&CK Tactics and Techniques** for a table of potential activity mapped to MITRE ATT&CK tactics and techniques.

Overview

Cybersecurity and Infrastructure Security Agency (CISA) and United States Coast Guard (USCG) analysts (collectively referred to as CISA in this report) conducted a threat hunt engagement at a critical infrastructure organization. During this hunt, CISA proactively searched for evidence of malicious activity or the presence of a malicious cyber actor on the customer's network using host, network, industrial control system (ICS), and commercial cloud and open-source analysis tools. CISA searched for evidence of activity by looking for specific exploitation tactics, techniques, and procedures (TTPs) and associated artifacts.

While CISA did not find evidence of threat actor presence on the organization's network, the team did identify several cybersecurity risks. These findings are listed below in order of risk. Technical details of each identified cyber risk are included, along with the potential impact from threat actor exploitation of each risk (recommendations for mitigating each risk are listed in the Mitigations section below).

Several of these findings align with those observed during similar engagements conducted by US Coast Guard Cyber Command (CGCYBER), which are documented in their 2024 Cyber Trends and Insights in the Marine Environment (CTIME) report. The authoring agencies encourage critical infrastructure organizations to review the CTIME report to understand trends in the techniques/attack paths threat actors are using to compromise at-risk organizations, and what mitigations organizations should implement to prevent a successful attack.

Key Findings

Shared Local Admin Accounts with Non-Unique Passwords Stored as Plaintext

Details: CISA identified a few local admin accounts with non-unique passwords; these accounts were shared across many hosts. The credentials for each account were stored plaintext in batch scripts. CISA discovered these authorized scripts were configured to create user accounts with local admin privileges and then set identical, non-expiring passwords—these passwords were stored in plaintext in the script. One script was configured to create an admin account (set with a password stored in the script in plaintext) and automatically add to the admin group. The account was set as the local admin account on many other hosts.

Potential Impact: The storage of local admin credentials in plaintext scripts across numerous hosts increases the risk of widespread unauthorized access, and the usage of non-unique passwords facilitates lateral movement throughout the network. Malicious actors with access to workstations with either of these batch scripts could obtain the passwords for these local admin accounts by searching the filesystem for strings like `net user /add`, identifying scripts containing usernames and passwords [T1552.001], and accessing these accounts to move laterally.

For example, during a controlled security validation exercise (with explicit permission from the customer), CISA used the credentials found in one of the scripts to log into its associated admin account locally on a workstation [T1078.003], and then establish a Remote Desktop Protocol (RDP) connection to another workstation [T1021.001]. This demonstrated that the credentials allowed local login to an admin account and enabled lateral movement to any workstation with the account. While using this account, the user had local admin privileges on many workstations. Upon initiating the RDP session, the system issued out a notification that another user was currently logged in and that continuing the session would disconnect the existing user, confirming that the account can be accessed remotely via RDP.

The uniform use of local admin accounts with identical, non-expiring passwords across numerous hosts, coupled with the storage of these credentials in plaintext within accessible scripts, elevates the risk of unauthorized access and lateral movement throughout the network.

With local admin access, malicious cyber actors can:

- Modify existing accounts or create new accounts [T1098], potentially escalating privileges or maintaining persistent access.
- Install malicious browser extensions on compromised systems [T1112].
- Communicate with compromised systems using standard application layer protocols [T1071], which may bypass certain security monitoring tools.
- Modify local policies to escalate privileges or disable security features [T1484].
- Alter system configurations or install software that executes at startup [T1547], ensuring continued access and persistence.
- Hijack the execution flow of applications to inject malicious code [T1574].

The widespread distribution of plaintext credentials and the use of identical passwords across hosts increases the risk of unauthorized access throughout the network. This vulnerability heightens the potential for attackers to conduct unauthorized activities, which may impact the confidentiality, integrity, and availability of the organization's assets.

Note: This finding was associated with workstations only; servers and other devices were not affected.

Insufficient Network Segmentation Configuration Between IT and Operational Technology Environments

Details: While assessing interconnectivity between the customer's IT and operational technology (OT) environments, CISA identified that the OT environment was not properly configured. Specifically, standard user accounts could directly access the supervisory control and data acquisition (SCADA) virtual local area network (VLAN) directly from IT hosts.

First, CISA determined it was possible to establish a connection via port 21 from a user workstation in the IT network to a system within the SCADA VLAN. The test established that a network path was available, the remote host was reachable, the port was open and listening for connections, and that the port was directly accessible between the IT and SCADA VLANs, with misconfigured network-level restrictions—for example, firewalls or access control lists (ACLs)—blocking the Transmission Control Protocol (TCP) connection on the

port. This test was conducted using a standard user account on a regular IT workstation without administrative privileges [T1078].

Second, CISA discovered that the customer did not have sufficient secured bastion hosts dedicated for accessing SCADA and heating, ventilation, and air conditioning (HVAC) systems. A bastion host—sometimes referred to as a jump box or jump server—is a specialized, highly secured system (often a server or dedicated workstation) that serves as the sole access point between a network segment (such as an internal IT network) and a protected internal network (like an OT or ICS environment). By inspecting and filtering all inbound and outbound traffic, a bastion host is designed to prevent unauthorized access and lateral movement, ensuring that only authenticated and authorized users can interact with internal systems. Though several hosts were designated as bastion hosts for remote access to SCADA and HVAC systems, they lacked the enhanced security configuration, dedicated monitoring, and specialized scrutiny expected of bastion hosts.

Potential Impact: Insufficient OT network segmentation configuration, network access control (NAC), and the ability of a non-privileged user within the IT network to use their credentials to access the critical SCADA VLAN [T1078] presents a security and safety risk. Given that SCADA and HVAC systems control physical processes, compromises of these systems can have real-world consequences, including risks to personnel safety, infrastructure integrity, and equipment functionality.

Malicious actors could further exploit potentially unsecured workstations with access to OT systems, and insufficient network segmentation configuration between IT and OT systems, in the following ways:

- Use RDP or Secure Shell (SSH) protocols to move laterally from compromised IT workstations to OT systems [T1021.001] [T1021.004].
- Execute commands and scripts using scripting languages like PowerShell to attack OT systems [T1059].
- Map network connections to identify paths to OT systems [T1049].
- Gather information about network configurations to plan attacks on OT systems [T1016].

By exploiting these weaknesses, attackers can potentially gain unauthorized access to critical OT systems, manipulate physical processes, disrupt operations, and cause harm.

Insufficient Log Retention and Implementation

Details: CISA was unable to hunt for every MITRE ATT&CK® procedure in the scoped hunt plan partly because the organization's event logging system was insufficient for this analysis. For example, Windows event logs from workstations were not being forwarded to the organization's security information event management (SIEM), verbose command line auditing was not enabled (meaning command line arguments were not being captured in Event ID 4688), logging in the SIEM was not as comprehensive as required for the analysis, and log retention did not allow for a thorough analysis of historical activity.

Potential Impact: The absence of comprehensive and detailed logs, along with a lack of an established baseline for normal network behavior, prevented CISA from performing thorough behavior and anomaly-based detection. This limitation hindered the ability to hunt for certain TTPs, such as living-off-the-land techniques, the use of valid accounts [T1078], and other TTPs used by sophisticated threat actors. Such techniques often do not produce discrete indicators of compromise or trigger alerts from antivirus

software, intrusion detection systems (IDS), or endpoint detection and response (EDR) solutions. Further, the lack of workstation logs in the organization's SIEM meant CISA could not analyze authentication events to identify anomalous activities, such as unauthorized access using local administrator credentials. This gap exposes networks to undetected lateral movement and unauthorized access.

Insufficient logging can prevent the detection of malicious activity by hindering investigations, which makes detection of threat actors more challenging and leaves the network susceptible to undetected threats.

Additional Findings

Misconfigured sslFlags on a Production Server

Details: CISA used PowerShell to examine the `ApplicationHost.config` file[1]—a central configuration file for Internet Information Services (IIS) that governs the behavior of the web server and its applications and websites—on a production IIS server. CISA observed an HTTPS binding configured with `sslFlags="0"`, which keeps IIS in its legacy "one-certificate-per-IP" mode. This mode disables modern certificate-management features, and because mutual Transport Layer Security (TLS) (client-certificate authentication) must be enabled separately in "SSL Settings" or by adding `<access sslFlags="Ssl, SslRequireCert" />`, the binding leaves the client-certificate enforcement off by default, allowing any TLS client to complete the handshake anonymously. Moreover, `sslFlags` does not control protocol or cipher selection, so outdated protocols or weak cipher suites (e.g., SSL 3.0, TLS 1.0/1.1) may still be accepted unless Secure Channel (Schannel)[2] has been explicitly hardened.

Potential Impact: The misconfigured `sslFlags` could enable threat actors to attempt an adversary-in-the-middle attack [T1557] to intercept credentials and data transmitted between clients and the IIS server. Malicious actors could also exploit vulnerabilities in older Secure Sockets Layer (SSL)/TLS protocols, as well as weak cipher suites, increasing the risk for protocol downgrade attacks in which an attacker forces the server and client to negotiate the use of weaker encryption standards [T1562.010]. This compromises the confidentiality and integrity of data transmitted over this channel. Furthermore, the absence of client certificate enforcement meant the server did not validate the identity of the connecting clients beyond the basic SSL/TLS handshake. This deficiency exposed the server to risks where unauthorized or malicious clients could impersonate legitimate users, potentially gaining access to sensitive resources without proper verification.

Misconfigured Structured Query Language Connections on a Production Server

Details: CISA reviewed `machine.config` file on a production server and identified that it was configured with a centralized database connection string, `LocalSqlServer`, for both profile and role providers. This configuration implies that, unless overridden in each application's `web.config` files, every ASP.NET site on the server connects to the same Structured Query Language (SQL) Express or `aspnetdb` database and shares the same credentials context.

---

[1] While CISA used PowerShell to review these configuration settings, they can also be identified by running a search in any text editor.
[2] For more information, see Schannel – Microsoft Learn.

Additionally, CISA identified that the `machine.config` file set the `minRequiredPasswordLength` to be less than 15 characters, which is CISA's recommended password length.

Potential Impact: Using a centralized database approach increases risk, as a single breach or misconfiguration in this central SQL database server can compromise all applications dependent on the server. This creates a single point of failure and could be exploited by attackers aiming to gain broad access to the system.

Additionally, setting the minimum password length to any password under 15 characters is more vulnerable to various forms of brute-force attacks, such as password guessing [T1110.001], cracking [T1110.002], spraying [T1110.003], and credential stuffing [T1110.004]. If a threat actor successfully cracked these weak passwords, they could gain unauthorized access to user or application accounts and leverage vulnerabilities within applications to further escalate privileges, potentially leading to unauthorized access to the backend SQL Server databases. This could result in data breaches, data manipulation, or a loss of database integrity.

Mitigations

CISA and USCG recommend that critical infrastructure organizations implement the mitigations below to improve their organization's cybersecurity posture. Recommendations to reduce cyber risk are listed for each of CISA's findings during this engagement and are ordered starting from the highest to lowest importance for organizations to implement. CISA and USCG also include general practices to strengthen cybersecurity for OT environments that are not tied to specific findings.

These mitigations align with the Cross-Sector Cybersecurity Performance Goals jointly developed by CISA and the National Institute for Standards and Technology (NIST). The Cybersecurity Performance Goals (CPGs) provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful TTPs. Visit CISA's CPGs webpage for more information.

Many of these mitigations also align with recommendations made by CGCYBER in their 2024 CTIME report. The report provides relevant information and lessons learned about cybersecurity risks gathered through operations similar to this threat hunt engagement, and best practices to mitigate these risks. Please see the 2024 CTIME report for additional recommendations for critical infrastructure organizations to implement to harden their environments against malicious activity.

Implement Unique Credentials and Access Control Measures for Administrator Accounts

- **Provision unique and complex credentials for local administrator accounts** [CPG 2.C] on all systems. Do not use shared or identical administrative credentials across systems. Ensure service accounts/machine accounts have passwords unique from all member user accounts.

  - For example, organizations can deploy Microsoft LAPS (see Microsoft Learn's Windows LAPS Overview for more information) to ensure each machine has a unique, complex local administrator password; passwords are rotated automatically within Microsoft Active Directory, reducing the window of vulnerability; and that password retrieval is limited to authorized personnel only.
- **Require phishing-resistant multifactor authentication (MFA) [CPG 2.H] in addition to unique passwords for all administrative access, including local- and domain-level administrator accounts,** RDP sessions, and VPN connections.
- **Use privileged access workstations (PAWs) dedicated solely for administrative tasks** and isolate them from the internet and general network to reduce exposure to threats and lateral movement.
  - Harden PAWs by applying CIS Benchmarks: limit software to essential administrative functions, disable unnecessary services and ports, and ensure regular updates and patches.
  - Enforce strict access controls to restrict PAW access to authorized administrators only.
- **Conduct continuous auditing of privileged accounts** by regularly collecting and analyzing logs of administrative activities, such as login attempts, command executions, and configuration changes [CPG 2.T].
  - Configure automated alerts for anomalous behaviors, including logins outside standard hours, access from unauthorized locations, and repeated failed logins.
  - Periodically review all administrator accounts to confirm the necessity and appropriateness of access levels; align these auditing practices with NIST SP 800-53 Rev. 5 Controls AU-2 (Auditable Events) and AU-12 (Audit Record Generation).
- **Apply the principle of least privilege** by limiting administrative privileges to the minimum required for users to perform their roles [CPG 2.E].
  - Create individual administrative accounts with unique credentials and role-specific permissions and disable or rename built-in local administrator accounts to reduce common attack vectors.
  - Avoid using shared administrator accounts to improve accountability and auditability, and ensure administrators use standard accounts for non-administrative tasks to minimize credential exposure.
  - Implement Role-Based Access Control (RBAC) to assign permissions based on job functions, as aligned with NIST SP 800-53 Rev. 5 Control AC-5 (Separation of Duties).
- **Identify and remove unauthorized or unnecessary local administrator accounts**, maintain oversight by documenting and tracking all authorized accounts, and enforce strict account management policies by restricting account creation privileges and implementing approval workflows for new administrator accounts.

Securely Store and Manage Credentials

- **Purge credentials from the System Center Configuration Manager (SCCM).** Review SCCM packages, task sequences, and scripts to ensure that no plaintext credentials are embedded, and update or remove any configurations that deploy scripts with plaintext credentials.

- **Do not store plaintext credentials in scripts**. Instead, store credentials in a secure manner, such as with a credential/password manager or vault, or other privileged account management solution [CPG 2.L].
  - Leverage SCCM's built-in capabilities to run tasks with administrative privileges without exposing credentials (for further guidance, refer to Microsoft's best practices for secure SCCM configuration).
- **Use encrypted communication**. If scripts must retrieve credentials at runtime, use encrypted channels and protocols (e.g., TLS 1.3) to communicate with secure credential stores. Ensure that credentials are not written to disk or exposed in logs.
- **Use unique local administrator passwords**, such as by deploying Microsoft LAPS. Set appropriate permissions on Active Directory attributes used by LAPS (`ms-MCS-AdmPwd` and `ms-MCS-AdmPwdExpirationTime`) per Microsoft's security recommendations.

Establish Network Segmentation Between IT and OT Environments

- **Assess the existing network architecture to ensure effective segmentation between the IT and OT networks** [CPG 2.F]—this process should evaluate both logical and physical segmentation, ensuring clear boundaries between IT and OT assets.
  - Use NIST SP 800-82 Rev. 3 (Guide to OT Security) and International Electrotechnical Commission (IEC) 62443 standards as guides for network segmentation best practices.
  - Network segmentation is essential for containing breaches within isolated segments and preventing them from spreading across networks. Depending on your environment, consider implementing the following segmentation:
    - Implement VLAN segmentation with inter-VLAN access controls.
    - Create separate VLANs for IT and OT systems, specifically isolating OT components such as SCADA systems from IT network VLANs.
    - Configure inter-VLAN access controls, including Layer 3 ACLs, to restrict traffic between IT and SCADA VLANs.
    - Deploy firewalls with application-layer filtering capabilities to monitor and control data flow between the VLANs, ensuring that only authorized protocols and devices can communicate across segments.
- **Implement a demilitarized zone (DMZ) between IT and OT environments** to provide an additional security layer.
  - Position firewalls at both the IT-DMZ and OT-DMZ boundaries to filter traffic and enforce strict communication policies.
  - Configure the DMZ to act as an intermediary, with only essential communications permitted between IT and OT networks.
  - Ensure the DMZ hosts shared services (e.g., bastion hosts, jump servers, or data historians) that require limited interaction with both environments, with access controls and monitoring in place.

- **Consider a full network re-architecture if current segmentation methods cannot effectively separate IT and OT networks.**
  - Collaborate with cybersecurity and network experts to design an architecture that meets ICS-specific security requirements—this redesign may involve transitioning to a micro-segmented or zero trust architecture, which includes strict identity verification for all users and devices attempting to access OT assets.[3]
- **Implement unidirectional gateways (data diodes)** where appropriate to prevent bidirectional communication.
- **Keep network diagrams, configuration files, and asset inventories up to date**.
- **Regularly test segmentation controls** to validate their effectiveness in restricting unauthorized access by conducting penetration testing and security assessments.
  - Include simulated breach scenarios to confirm that segmentation contains threats within isolated zones.
  - Ensure compliance with NIST SP 800-53 Rev. 5 Control AC-4 (Information Flow Enforcement) to align segmentation measures with best practices for controlled information flow.

Prevent Unauthorized Access via Port 21

- **Disable File Transfer Protocol (FTP) services on SCADA devices and servers if they are not required.** Replace FTP with secure alternatives, such as SSH FTP (SFTP) or FTP over TLS/SSL (FTPS).
- **Block inbound and outbound FTP traffic on port 21 using firewalls and ACLs**.
  - Implement restrictive ACL policies at network boundaries to control FTP access across all network layers.
  - As outlined in CIS Control 9.2 (Limit Unnecessary Ports, Protocols, and Services), close any unused ports to strengthen network defenses.
- **Implement IDS/Intrusion Prevention System (IPS) technologies to monitor traffic between the IT network and SCADA VLAN**, use signature and anomaly detection, and integrate IDS/IPS with a SIEM system for centralized monitoring.
- **Enhance authentication and encryption mechanisms**. Require MFA for SCADA access, use secure remote access technologies when necessary, securely encrypt communications (using protocols such as TLS 1.2 or higher, preferably TLS 1.3), and establish VPN tunnels to communicate between IT networks and SCADA systems.
- **Perform network traffic filtering and deep packet inspection.**
  - Use SCADA-aware firewalls capable of understanding SCADA protocols and inspecting and filtering traffic at the application layer.

[3] Reference the Purdue Model for ICS Security as a guide for layered security zones and assess compliance with IEC 62443 network and system security standards; organizations may use this version of the model developed by Department of Energy (DOE) as a guide: Purdue Model Framework for Industrial Control Systems & Cybersecurity Segmentation.

- Only allowlist authorized protocols and command structures to SCADA operations. Use one-way communication devices to prevent data from flowing back into the SCADA network.

Establish Secure Bastion Hosts for OT Network Access

- **Ensure bastion hosts are dedicated secure access points** exclusively used to access the OT network and deployed as **exclusive management gateways for all devices within a network**.
  - Make bastion hosts the single access points for conducting all administrative tasks, system management, and configuration changes; this centralizes access control and ensures any interaction with the OT system passes through a rigorously monitored and secure environment, minimizing the potential for unauthorized access.
- **Do not allow staff to use bastion hosts as regular workstations**.
  - Provide staff with separate workstations for accessing email, internet browsing, etc., on the IT network.
  - Establish and enforce policies that prohibit non-administrative activities on bastion hosts, ensuring they remain dedicated to OT network access.
- **Regularly audit and monitor bastion hosts** to maintain security integrity, prevent unauthorized use, and quickly address any vulnerabilities or policy non-compliance.
- **Configure comprehensive logging of all activities on bastion hosts**, including authentication attempts, command executions, configuration changes, and file transfers. Aggregate logs into a SIEM.
- **Isolate bastion hosts from the IT network**; bastion hosts should reside in a separate security zone with restricted communication pathways (see CISA's infographic on Layering Network Security Through Segmentation).
  - Deploy bastion hosts in a DMZ, imposing physical and logical isolation from other networks.
  - Configure firewalls between the IT network, bastion hosts, and the OT network, enforcing strict access control policies to allow only necessary traffic.
- **Ensure secure configuration and hardening of bastion hosts:** Comply with NIST SP 800-123 and CIS Benchmarks and CNSSI 4009-2015, remove nonessential applications and services to reduce the attack surface, configure system settings to be secure, conduct effective patch management, enforce the principle of least functionality, and disable unused ports and protocols.
- **Implement access control policies:** remove any access permissions to the OT network from IT workstations and ensure only bastion hosts have access to the OT network.
  - Implement NAC solutions to enforce policy-driven access control decisions based on device compliance and user authentication to provide dynamic access control and real-time visibility into the devices on the network.
- **Equip each bastion host with robust authentication mechanisms,** including phishing resistant MFA [CPG 2.H], to verify the identity of users accessing the network.
  - Align with AAL3 as defined in NIST SP 800-63B. AAL3 requires hardware-based authenticators and proof of possession of cryptographic keys through secure authentication protocols.

- **Implement stringent access controls that restrict access to authorized personnel only using RBAC principles**, ensuring that personnel can only access information and perform tasks pertinent to their roles and duties. This reduces the risk of internal threats or lateral movement and prevents unauthorized access.
- **Securely configure remote access tools**, including by using secure protocols and disabling remote access tools on IT workstations to the OT network, enforcing that all remote access occurs through bastion hosts.
  - Disable insecure protocols like Telnet and unencrypted VNC to prevent interception and unauthorized access.
  - Log all remote access sessions and monitor for unauthorized or anomalous activities.

Implement Comprehensive Logging, Log Retention, and Analysis

- **Implement comprehensive and verbose (i.e., detailed) logging across all systems**, including workstations, servers, network devices, and security appliances [CPG 2.T].
  - Enable logging of critical events such as authentication attempts, command-line executions with command arguments (Event ID `4688`), and network connections.
- **Aggregate logs in an out-of-band, centralized location** [CPG 2.U] where adversaries cannot tamper with them, such as a dedicated SIEM, in order to facilitate behavior analytics, anomaly detection, and proactive threat hunting [CPG 2.T, 2.U]. For more information on behavior- and anomaly-based detection techniques, see joint guidance Identifying and Mitigating Living off the Land.
- **Ensure comprehensive logging on bastion hosts for all activities.** Capture detailed records of login attempts [CPG 2.G], commands executed (with command arguments enabled), configurations changed, and files transferred.
  - Integrate bastion hosts with a centralized SIEM (NIST SP 800-137).
- **Continuously monitor logs** for early detection of anomalous activities. Configure the SIEM to generate automatic alerts for suspicious activity and implement behavior analysis techniques to detect anomalies.
- **Securely store log backups and use tamper resistant storage** [CPG 2.U] to prevent a threat actor from altering or purging logs to conceal malicious activity.

For additional guidance on logging, see joint guidance Best Practices for Event Logging and Threat Detection.

Securely Configure HTTPS Bindings and LocalSqlServer Connection String

- Enforce both client certificate verification and secure renegotiation in IIS by configuring the `sslFlags` setting to `"3"` in the `ApplicationHost.config` file. Setting `sslFlags="3"` requires clients to present valid `X.509` certificates for authentication and implements the TLS Renegotiation Indication Extension (RFC 5746). To implement this, perform the following steps:
  - Locate the `<binding>` element for the HTTPS site within `ApplicationHost.config`.
  - Set the `sslFlags` attribute to `"3"`: `<binding protocol="https" bindingInformation="*:443:" sslFlags="3" />`.

- Restart IIS to apply the changes: `iisreset`.

- **Restrict the server to use only secure and up-to-date SSL/TLS protocols and cipher suites.**
  - Disable deprecated protocols like SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.1 to prevent protocol downgrade attacks that compromise the confidentiality and integrity of data.
- **Override the global settings in `machine.config`** by modifying each application's `web.config` file to define its own connection strings and providers. This isolates applications at the database level and allows for tailored security configurations for each application.
- **Create dedicated SQL Server database accounts for each application with permissions limited to necessary operations** (e.g., SELECT, INSERT, UPDATE), and avoid granting excessive privileges.
  - Do not assign roles like `db_owner` or `sysadmin` to application accounts. This reduces the risk of privilege escalation and enhances accountability through segregated access logs.
- **Use `machine.config` only for configurations that must be applied globally** across all applications on the server.
  - Audit the `machine.config` file to ensure no application-specific settings are present.

Enforce Strong Password Policies

- **Implement a system-enforced policy that requires a minimum password length of 15 or more characters** for all password-protected IT assets and all OT assets, when technically feasible [CPG 2.B].
  - **Consider leveraging passphrases and password managers** to make it easier for users to maintain sufficiently long passwords.
- In instances where minimum password lengths are not technically feasible, **apply and record compensating controls**, such as rate-limiting login attempts, account lockout thresholds, and strong network segmentation. Prioritize these systems for upgrade or replacement.
- **Implement MFA** [CPG 2.H] in addition to strong passwords (i.e., passwords 15 characters or longer).

Additional Mitigation Recommendations to Strengthen Cybersecurity

CISA and USCG recommend critical infrastructure organizations implement the following additional mitigations (not tied to specific findings from the engagement) to improve the cybersecurity of their IT and OT environments:

- **Secure RDP from the IT to OT environments by deploying dedicated VPNs for all remote interactions with the OT network**. Using RDP without strong authentication practices can lead to credential theft. Additionally, RDP does not inherently segregate or closely monitor user sessions, which can allow a compromised session to affect other parts of the network.
  - **Deploy VPNs with strong encryption protocols such as SSL/TLS or Internet Protocol Security (IPsec)** [CPG 2.K] to safeguard data integrity and confidentiality; use MFA [CPG 2.H] at all VPN access points to ensure only authorized personnel can gain access.

- **Configure VPN gateways to perform rigorous security checks and manage traffic destined for the OT network**, ensuring comprehensive validation of all communications through pre-defined security policies.
  - VPN gateways should function as the primary enforcement points for access controls, scrutinizing every data packet to detect and block unauthorized access attempts.
- Align the VPN traffic monitoring with the DMZ's capabilities to **regulate and inspect the data flow between IT and OT environments**.
- As part of the broader network architecture review, **ensure the VPN infrastructure is correctly segmented from other network resources** [CPG 2.F] to prevent any spillover effects from the IT environment to the OT network, containing potential breaches within isolated network zones.
- **Within the VPN configuration, enforce strict routing rules that require all remote access requests to pass through the DMZ and be authenticated by bastion hosts**. This minimizes the risk of unauthorized access and ensures that all remote interactions with the OT network are monitored and controlled.

- If wireless technology is employed within the OT environment, **implement Wi-fi Protected Access 3 (WPA3)-Enterprise encryption with strong authentication protocols like Extensible Authentication Protocol (EAP)-TLS** to ensure data confidentiality and integrity.
  - Deploy and continuously monitor Wireless Intrusion Prevention Systems (WIPS) to detect, prevent, and respond to unauthorized access attempts and anomalous activities within the wireless network infrastructure.
  - Disable unnecessary features like Service Set Identifier (SSID) broadcasting and peer-to-peer networking, enable Media Access Control (MAC) filtering as an additional layer, and keep wireless firmware updated.

Validate Security Controls

In addition to applying mitigations, CISA and USCG recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. CISA and USCG recommend testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see **Table 1** to **Table 9**).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program—including people, processes, and technologies—based on the data generated by this process.

CISA and USCG recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

Contact Information

Critical infrastructure organizations are encouraged to report suspicious or criminal activity related to information in this advisory to:

- CISA via CISA's 24/7 Operations Center (SOC@mail.cisa.dhs.gov or 888-282-0870) or your local FBI field office. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.
- Coast Guard, for Maritime Transportation System Subsector organizations. Report malicious activities to the Coast Guard's National Response Center (1-800-424-8802) per Navigation and Vessel Inspection Circular (NVIC) 02-24 when facilities observe any unusual activity or interruptions to their network. For additional Coast Guard resources, please visit the Coast Guard Maritime Industry Cybersecurity Resource Center website. CGCYBER can also be contacted at maritimecyber@uscg.mil.

Additional Resources

For more information on improving cyber hygiene for critical infrastructure IT and OT environments, please see the following additional resources authored by CISA, CGCYBER, and international partners:

- CGCYBER 2024 CTIME report
- Joint Guidance Best Practices for Event Logging and Threat Detection
- Joint Guidance Principles of Operational Technology Cyber Security

Disclaimer

The information in this report is being provided "as is" for informational purposes only. CISA and USCG 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 USCG.

Version History

July 31, 2025: Initial version.

Appendix: MITRE ATT&CK Tactics and Techniques

See **Table 1** to **Table 9** for all referenced threat actor tactics and techniques in this advisory. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.

Table 1: Initial Access

Technique Title	ID	Use
Valid Accounts	T1078	Malicious actors could use access to valid accounts for access to IT and OT networks.
Valid Accounts: Local Accounts	T1078.003	Threat actors could use credentials obtained for local administrator accounts to gain administrator access to workstations or services that use the account.
Account Manipulation	T1098	Malicious actors could modify existing accounts or create new accounts to maintain access or escalate privileges.

Table 2: Execution

Technique Title	ID	Use
Command and Scripting Interpreter	T1059	Malicious actors could use script interpreters like PowerShell to execute commands and scripts.

Table 3: Persistence

Technique Title	ID	Use
Boot or Autostart Execution	T1547	Malicious actors could configure `autostart` execution paths to ensure persistence.
Hijack Execution Flow	T1574	Malicious actors could hijack the execution flow of applications and inject malicious code.

Table 4: Privilege Escalation

Technique Title	ID	Use
Domain or Tenant Policy Modification	T1484	Malicious actors could modify domain policies to escalate privileges or evade defenses.

Table 5: Defense Evasion

Technique Title	ID	Use
Modify Registry	T1112	Malicious actors could install malicious browser extensions on compromised systems.
Impair Defenses: Downgrade Attack	T1562.010	Malicious actors could exploit vulnerabilities in older systems to force a downgrade to a less secure mode of operation.

Table 6: Credential Access

Technique Title	ID	Use
Unsecured Credentials: Credentials in Files	T1552.001	Malicious actors could search for and exploit credentials stored in unsecured files.
OS Credential Dumping	T1003	Malicious actors could extract credentials from memory or storage from unsecured workstations.
Adversary-in-the-Middle	T1557	Malicious actors could position themselves between networked devices to intercept credentials and other data.
Brute Force: Password Guessing	T1110.001	Malicious actors could systematically guess possible passwords.
Brute Force: Password Cracking	T1110.002	Malicious actors could recover plaintext credentials after obtaining password hashes or other similar credential material.
Brute Force: Password Spraying	T1110.003	Malicious actors could attempt to use a common password against different accounts to try to obtain account access.
Brute Force: Credential Stuffing	T1110.004	Malicious actors could try to use credentials gained from an unrelated account to gain access to a desired account in the victim's environment.

Table 7: Discovery

Technique Title	ID	Use
System Network Connections Discovery	T1049	Malicious actors could map network connections to identify paths to OT systems from an unsecured IT workstation with access to the OT network.
System Network Configuration Discovery	T1016	Malicious actors could use an unsecured workstation to discover network configurations.

Table 8: Lateral Movement

Technique Title	ID	Use
Remote Services: Remote Desktop Protocol	T1021.001	Malicious actors could use valid credentials to establish an RDP connection to access a workstation.
Remote Services: SSH	T1021.004	Malicious actors could use valid accounts to establish an SSH connection to a workstation.

Table 9: Command and Control

Technique Title	ID	Use
Application Layer Protocol	T1071	Malicious actors could use application layer protocols to communicate with systems they compromised while blending in with existing network traffic.