Confidence in the Connected World

Center for Internet Security®

CIS Controls™

Version 7

Implementation Guide

for Industrial Control Systems

Contents

Acknowledgements

CIS® (Center for Internet Security, Inc.) would like to thank the many security experts who volunteer their time and talent to support the CIS Controls™ and other CIS work. CIS products represent the effort of a veritable army of volunteers from across the industry, generously giving their time and talent in the name of a more secure online experience for everyone.

Editors:

Ramsey Williams, Sr. Director – GE Digital, Cyber Security
Adam Boeckman, Great Bay Software, Cybersecurity Engineer Specialist, CEH and GICSP

Contributors:

Andy Gaither, NV Energy, Manager of Operations Technology
Scott King, Rapid 7, Sr. Director, Advisory Services
Darren Bennet, City of San Diego; Chief Information Security Officer
Joshua Carlson, Schneider Electric; SME and Technical Sales Leader, Cybersecurity
Shane Markley, Southwest Gas, Cybersecurity Operations Team Lead
Patrick Norton, Tampa Bay Water;
SANS Institute ICS Curriculum Team;
Ted Gary, Tenable, Sr. Product Marketing Manager
Cody Dumont, Tenable, Information Security Content Manager

Introduction

The CIS Critical Security Controls® (CIS Controls®) are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. The CIS Controls are developed by a community of IT experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the CIS Controls come from a wide range of sectors including, retail, manufacturing, healthcare, education, government, defense, and others. So, while the CIS Controls address the general practices that most organizations should take to secure their systems, some operational environments may present unique requirements not addressed by the CIS Controls.

The security challenges facing Industrial Controls Systems (ICS) are one such example where additional attention is required. While many of the core security concerns of enterprise IT systems are shared by ICS operators, the main challenge in applying best practices to ICS is tied to the fact that these systems typically operate software and hardware that directly control physical equipment or processes. Compounding this issue is the fact that many of systems not only often have high availability requirements, but also are often the underpinning of critical infrastructure.

CIS (Center for Internet Security, Inc.) is a 501c3 non-profit organization whose mission is to identify, develop, validate, promote, and sustain best practices in cybersecurity; deliver world-class cybersecurity solutions to prevent and rapidly respond to cyber incidents; and build and lead communities to enable an environment of trust in cyberspace.

For additional information, go to

Operational Technology (OT) teams often rely heavily on vendor technologies, products, systems, and services. Many ICS vendor systems are designed and deployed using combinations of open and proprietary technologies and it's not uncommon for an ICS, once installed, to be accompanied with warrantees and guarantees of that system's reliability and performance. These types of agreements are sometimes deemed critical by ICS asset owners since they help provide added assurance of the system's operational integrity, while they can also aid in cost-recovery associated with system downtime. ICS vendors often provide such agreements as a way to assume or offset aspects of risk as an automation and control system supplier to an asset owner. Such agreements are offered because the vendors conduct extensive engineering, testing, and validation of software and hardware combinations in these systems to help rule out potential compatibility and interoperability issues that may impact ICS operation. However, such agreements often place restrictions on ICS asset owners for what adjustments they can make to an ICS without voiding such a warranty. In some cases, even the addition of a simple security control to an ICS, or a minor configuration change can void a warranty. Therefore, these agreements must be considered when determining how to best implement critical security controls to an ICS.

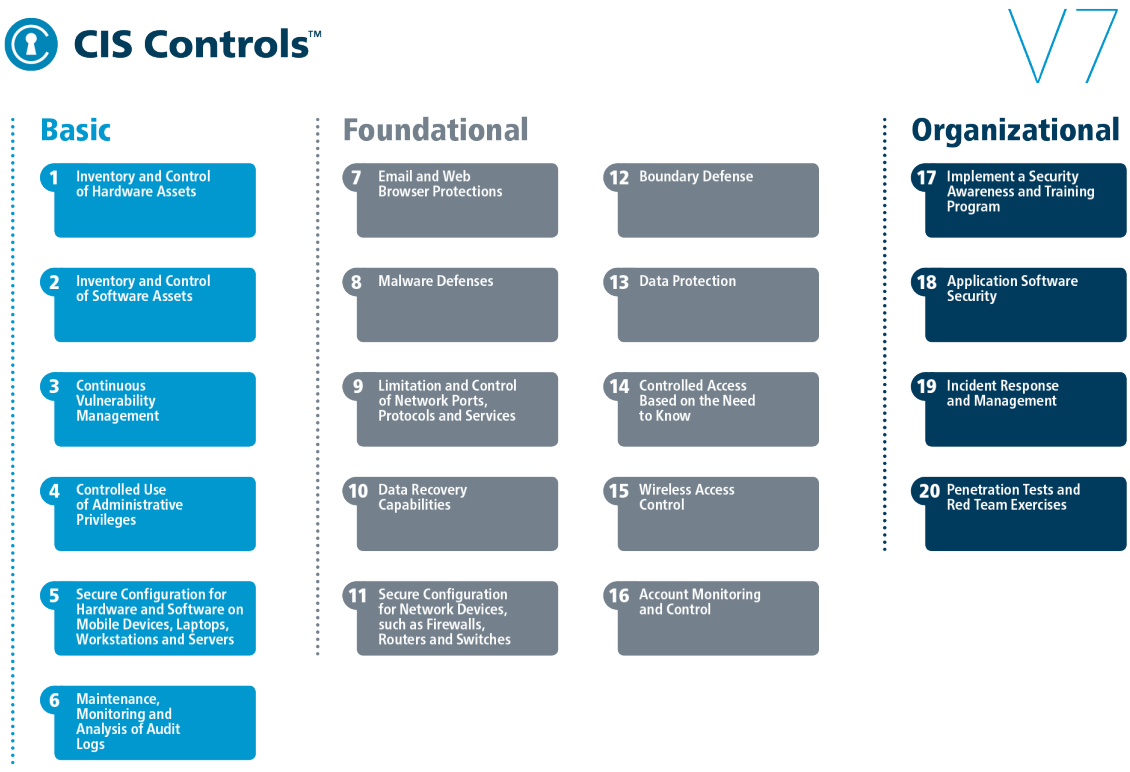
ICS environments may also have many embedded IP connected devices. These devices often lack the capability to support traditional Information Technology (IT)-grade security control technologies since many run specialized firmware and Real-time Operating Systems (RTOS), utilize proprietary protocols such as Profibus, COTP, TPKT Modbus, and EtherNet/IP, or do not have the capability to support contemporary endpoint or supplicant software that is commonly used in IT systems. Additionally, for ICS, the primary security focus tends towards ensuring operational integrity in the systems, rather than to data protection and privacy. Therefore, availability is a primary concern when developing a security program to address an organization's risk associated with its OT systems.

Consisting of a combination of routable and non-routable communication paths, ICS network architectures often differ from traditional Information Technology (IT) environments. The overriding themes for applying security for ICS are segmentation and boundary control between the IT and OT domains, and careful controls around local and remote connectivity to reduce attack vectors that threat actors can utilize to gain access to ICS networks.

How to Use this Document

In this document, we provide guidance on how to apply the security best practices found in CIS Controls Version 7[1] to ICS environments. For each top-level CIS Control, there is a brief discussion of how to interpret and apply the CIS Control in such environments, along with any unique considerations or differences from common IT environments. The applicability or not of specific Sub-Controls is addressed and additional steps needed in ICS environments are explained. Throughout this document, we take into consideration the unique mission/business requirements found in ICS environments (with a focus on performance and real-time requirements), as well as the unique risks (vulnerabilities, threats, and consequences), which in turn drive the priority of the security requirements (e.g., availability, integrity, and confidentiality of process data).

By walking through CIS Controls Version 7 with this Companion document, the reader should be able to tailor the CIS Controls in the context of a specific IT/OT enterprise as an essential starting point for a security improvement assessment and roadmap.



[1] The newest version of the CIS Controls and other complementary documents may be found at www.cisecurity.org.

CIS Controls (Version 7): ICS Security

CIS Control 1 – Inventory and Control of Hardware Assets	
ICS Rationale, Applicability, and Considerations	
Introduction	The first CIS Control is considered to be the most important because it's necessary to first identify the systems and devices that need to be secured. CIS Control 1 is about taking inventory. Understanding and solving the asset inventory and device visibility problem is critical in managing a business' security program. This is especially challenging in ICS where network segmentation, dual-homing, and isolation are common themes. Mixtures of old and new devices from multiple vendors, lack of up-to-date diagrams, unique industry, and application-specific protocols, some of which are not IP-based, and the difficulty in conducting physical inventories in dispersed or hostile environments compound these challenges.
Applicability	The conventional approach of using ping responses, TCP SYN or ACK scans can also be problematic in ICS due to device sensitivity since even seemingly benign scanning employed in IT environments can disrupt communications, or in some cases even impact device operations. Methods that are more passive to locate connected assets are preferred, as they are less likely to impact system availability or interact with vendor systems in a manner that could cause warranty issues. Where practical, non-intrusive methods should be leveraged including MAC-ARP tables, DNS, active directory, or a variety of ICS-specific tools employed to control and collect data in these systems all for the purpose of locating the variety of connected assets. Network level authentication via 802.1x does not work on many of the devices found in ICS, which do not support supplicant software. Network level authentication can cause reliability issues if not strictly maintained. Instead, consider a non-802.1x network access approach that is more ICS device-friendly and can at a minimum alert of new devices detected on the network. • Sub-Controls related to network level authentication may not be applicable to ICS environments. • Sub-Controls related to client-based certificates may not be applicable to ICS environments. • Certificate-based authentications in PKI environments can be complex and expensive.
Considerations	For this CIS Control consider the following additional steps: • Consider the lifecycle and acquisition costs, for example, NIST 800-82r2: Component Lifetime. Typical IT components have a lifetime on the order of 3 to 5 years, with brevity due to the quick evolution of technology. For ICS, where technology has been developed for very specific use and implementation, the lifetime of the deployed technology is often 10 to 15 years and sometimes longer. • Ensure that all equipment acquisitions and system modifications follow an approval process and the technical drawings (if applicable, automated inventory systems) are updated at the time of the change.

CIS Control 2 – Inventory and Control of Software Assets	
ICS Rationale, Applicability, and Considerations	
Introduction	This CIS Control offers steps needed to identify, track, and account for software in a network. Actively managing software can be a challenge in ICS. Much of the software is provided by vendors and is tied to hardware levels. This software often has commercially available components that are also tied to the hardware. Furthermore, applying patches to the operating systems and software applications can introduce new variables that lead to incompatibilities and even disruption or potential for loss or damage to data, product, equipment, and the safety of personnel. Using automated software inventory tools can also pose a challenge in ICS. Many collection methods rely on active scanning or endpoint software. Large parts of ICS networks are comprised of devices too sensitive to scan or unable to support endpoint software.
Applicability	Sub-Controls related to air gapped systems and network isolation may not be applicable. Due to the network communication requirements of many ICS software, true isolation may not be possible. Additionally, depending on OEM vendor offering and support, virtualization may not be supported. Instead, utilize transparent firewalls or subnet-wide segmentation to mitigate high-risk applications. Exercise caution when considering automated software inventory tools as these may cause stability issues on some systems. Many ICS devices may not support or be too sensitive to these tool's collection methods. For Sub-Control(s) related to whitelisting, utilize application whitelisting technology only where feasible. Depending on system criticality, unauthorized software can be alerted or blocked from executing on systems. For embedded devices that utilize firmware, leverage firmware signing (or something similar) if available.
Considerations	For this CIS Control consider the following additional steps: • Ensure ICS manufacturers and vendors provide a list of recommended and supported software and versions that are required for each system. • Forecast operating systems and application lifecycle cost in alignment with typical COTS (commercial off the shelf software) End of Life and End of Support (EoL/EoS) Notifications. • Ensure cybersecurity requirements are a consideration within procurement/sourcing processes. Specifically, ensure vendors leverage a secure development lifecycle.

CIS Control 3 – Continuous Vulnerability Management	
ICS Rationale, Applicability, and Considerations	
Introduction	This CIS Control addresses the need for continuous vulnerability management, which can be a significant task in most organizations. Understanding and managing vulnerabilities is just as challenging to an ICS environment as it is to traditional IT systems. One advantage the ICS has in this arena is that these systems typically reside farther into a business's network layers making it harder for external threat actors to reach and exploit new vulnerabilities without first telegraphing some presence inside the system when monitoring is in place. However, the required up-time on ICS means that the service and maintenance windows where updates can be applied are limited and sometimes months (or years) apart. Additionally, differences in ICS lifecycle and vendor support can overlap with software obsolescence, causing periods where no updates exist. These scenarios should be identified as part of the vulnerability scanning control and mitigations or upgrade plans should be put into place.
Applicability	Sub-Controls(s) related to automated scanning and patching may not be applicable in the ICS environment.
Considerations	When performing active vulnerability scanning, caution should be exercised as it can adversely affect ICS network communications and in-turn, product and system availability. There are several reasons for this, including network stack sensitivity, limited resources, or other situational factors. Scanning should only take place during process outages such as regular schedule maintenance or during planned shutdowns. Furthermore, steps should be taken (example: reboot or restart critical services) to ensure there are no unintended side effects. Ensure that tools do not automatically deploy software. These tools should report and identify where security updates are needed, but allow the OT team to deploy updates when it is safe to do so. For this CIS Control consider the following additional steps: • In addition to traditional channels, utilize an OEM vulnerability reporting service to identify all known vulnerabilities on the organization's ICS. • Utilize passive monitoring tools which identify a specific device and software version and correlate that to known vulnerabilities. • Operating system and application updates, security patches, and service packs need to be properly regression tested to ensure availability and reliability of the system will not be adversely affected. Where possible, have OEM regression test completed prior OT team testing. • Create a test bed that mimics a production environment for specific patch regression testing prior to implementing in production OT environments.

CIS Control 4 – Controlled Use of Administrative Privileges	
ICS Rationale, Applicability, and Considerations	
Introduction	This CIS Control addresses the need for limiting and managing administrator access. One of the two primary ways for attackers to spread inside a system is by tricking a user with elevated credentials into opening an email attachment, downloading and running infected file, or visiting a malicious website from an asset connected to the ICS. As per Control 7, these externally-enabled attack vectors should not be present on ICS networks. The method of guessing or cracking a password is still a valid concern, especially due to older devices that lack adequately engineered authentication and authorization mechanisms that recognize and protect against brute force attacks. Because of these differences, a handful of Sub-Controls should not be implemented in an ICS environment.
Applicability	Sub-Controls related to the use of multi-factor authentication may be possible for crossing boundaries, but may not be possible with the internal ICS environment. Sub-Controls related to the use of automated tools that alert when new users are added may not be applicable. Sub-Controls related to the use of dedicated machines or the use of isolation for administrator machines may not be applicable. When inventorying all administrative accounts, automated tools are not required and should only be used if known to not impact system availability. Typically account validation is performed by a system owner as opposed to a senior executive. When implementing a password policy, accounts with administrative privileges should be required to use long (14+ character) passwords or passphrases. Passphrases are typically words strung together with or without character complexity. This added length adds significant resilience to character guessing and cracking techniques. Default accounts that require administrative access and risks associated with altering those accounts should be reviewed and verify all changes with vendor prior to changes.
Considerations	For this CIS Control consider the following additional steps: • Minimize the use of elevated privileges and only use administrative accounts where they are required.

CIS Control 5 – Secure Configurations for Hardware and Software on Devices, Laptops, Workstations, and Servers	
ICS Rationale, Applicability, and Considerations	
Introduction	This CIS Control provides guidance for securing hardware and software. Many modern ICS logic and visualization platforms operate on common operating systems and many benchmarks and hardening guides exist. It is also important to also consider OEM and vendor recommendations in terms of standard security configuration for all manufacturer-provided operating systems and software. Additionally, many ICS devices do not fit into the categories mentioned in CIS Control 3 or 11 but should still have some level of secure configurations. At a minimum, and where possible, these devices should have unused services and ports disabled, default accounts changed, and protocols updated, and be examined for other ways to reduce the devices' attack surface. When this is not possible, monitoring should be employed as a means to detect and alert on unusual activities that may be suspect.
Applicability	All the Sub-Controls are applicable.
Considerations	It is recommended that when configuration management tools are used, they be set to alert-only without automated configuration re-deployment unless it is known to be safe to do so.

CIS Control 6 – Maintenance, Monitoring, and Analysis of Audit Logs	
ICS Rationale, Applicability, and Considerations	
Introduction	This CIS Control offers guidance for the maintenance and monitoring of audit logs. Logging of security events in ICS environments can be a challenge due to the nature of many of the embedded or legacy devices present. Many devices do not support native logging of security events. Those that do often do not inherently support sending those events to an external device such as a central logging server so special action may need to be taken to gain access to such information.
Applicability	All Sub-Controls are applicable. However, many systems or devices may not support the level of logging recommended by this Control.
Considerations	If looking to leverage an IT-based SIEM, make sure it supports the ICS environment because many logging analytic and alerting solutions do not support or correctly interpret or correlate ICS specific events.

CIS Control 7 – Email and Web Browser Protections	
ICS Rationale, Applicability, and Considerations	
Introduction	This CIS Control focuses on the security of web browsers and email clients, which are very vulnerable attack vectors. Most ICS environments do not require Internet web access and email clients are not needed because they are often isolated from business networks. Email is utilized in ICS environments but typically only in an outgoing manner. It is common to have systems that monitor critical processes send out alerts or reports via email. These emails are typically accessed from business or corporate assets that are on separate networks and have no access to the ICS environment. While Internet web access is not required, often services are provided via internal web servers. Therefore, unlike email clients, web browsers may still be required, but the risk posed by these browsers is greatly reduced as an attacker would have to first compromise the internal web server.
Applicability	Most of the Sub-Controls are not applicable to the ICS environment for the reasons stated above. However, Sub-Controls related to using authorized browsers for business purposes are applicable. The key is restricting web access.
Considerations	In cases where certain Sub-Controls are not applicable, the following additional requirements should be enforced: • Ensure that all systems are segmented such that there is no Internet web access. • Ensure that no email clients are installed or present on any systems. Where a device or system has the capability to send email-based alerts or reports, ensure that it is limited to outbound only.

CIS Control 8 – Malware Defenses	
ICS Rationale, Applicability, and Considerations	
Introduction	This CIS Control addresses the steps needed to ensure a strong defense against malware intrusions. Malicious code is a very real threat to ICS. It has been crafted to target the devices or processes unique to these industries. While proper network segmentation and defense-in-depth strategies help to mitigate this risk by making it difficult for threat actors to deliver malware to their intended locations, malware defense still needs tools and processes in place to detect incidents. Unfortunately, the sensitivity and critical nature of these environments make it difficult to regularly update Antivirus definitions for the fear the update process might impact the reliability of critical systems. Additionally, many devices do not support endpoint software, thus making on-device malware monitoring difficult.
Applicability	All Sub-Controls are applicable.
Considerations	For this CIS Control consider the following additional steps: • Anti-malware tools need to be properly regression-tested to ensure that availability and reliability of the system will not be adversely affected. This testing should take place whenever a change is made to the anti-malware software such as a configuration change, software hotfix, or repository update. • Ensure anti-malware tools are configured such that a false positive detection will not negatively impact the availability or reliability of any critical processes. Some OT teams may not want to incur the risk of updating antivirus definitions while critical processes are running. Consider, at a minimum, performing software updates to scanning engines and signature databases during scheduled maintenance or outages. When scanning removable media, it is recommended that the content be scanned before it can be accessed, but not upon insertion. By scanning on insertion, larger portable storage devices can take a significant time to finish scanning and impede productivity. However, by scanning prior to access, content can be scanned on demand and have less of an impact on productivity. Anti-exploitation features can be very challenging to implement. Much of the industry's proprietary software has not been designed to leverage operating systems' memory protection features. Other devices simply cannot support these technologies. Some third-party packages can enable anti-exploitation functionality to supported devices. However, they can often create resource overhead that may impact the real-time requirements of these systems. While anti-exploitation technologies are valuable, they should only be applied where they are innately supported or do not impact the performance of ICS.

CIS Control 9 – Limitations and Control of Network Ports, Protocols, and Services	
ICS Rationale, Applicability, and Considerations	
Introduction	This CIS Control focuses on the need for controlling network access points, ports, and services. When accounting for ports, protocols and services, it is often helpful to start from vendor documentation since many ICS comprise proprietary systems. Many vendors or OEM have baseline documentation that can provide a starting point or details specific to their solutions.
Applicability	All the Sub-Controls are applicable.
Considerations	When inventorying open or available network ports, the process or tools used should be non-intrusive and not impact the availability or reliability of the system. In the ICS environment, most systems are considered critical and mail servers should not be present in ICS networks.

CIS Control 10 – Data Recovery Capabilities	
ICS Rationale, Applicability, and Considerations	
Introduction	This CIS Control references the need for performing system backups for data recovery capability. It requires different approaches within individual ICS environments. Different components support various backup methods. While some support full system backups, the majority offer only configuration exports. Still others may offer no capability to export configurations.
Applicability	All the Sub-Controls are applicable.
Considerations	For this CIS Control consider the following additional steps: • Ensure that system backups and recovery procedures are documented. In terms of back-ups, most ICS systems do not support complete automatic backups, and the scheduling of these backups might cause ICS performance. Where this is the case, ensure backups are taken as appropriate. Additionally, some device configurations remain static and rarely change. In these situations, backups may only need to be performed when configurations or data changes are made. Nonetheless, it remains important to evaluate even configurations that are expected to remain unchanged because any alteration could be an indicator of accidental/unintentional alteration, tampering or malicious intent. In cases where devices are not capable of complete backups, all software, settings, and configurations should be captured such that all information necessary to perform a restoration is known and available.

CIS Control 11 – Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	
ICS Rationale, Applicability, and Considerations	
Introduction	This CIS Control addresses the need to manage the configuration of all network devices using a change control process. The network infrastructure of an ICS network typically carries additional requirements when compared to traditional IT systems. Usually these networks focus on availability and are architected with real-time performance and redundancy requirements. Attack vectors, however, remain the same. Unsecure services, poor firewall configurations, and default credentials remain issues.
Applicability	Due to the availability requirements associated with the ICS environments, Sub-Controls relating to network traffic may not be applicable.
Considerations	For this CIS Control consider the following additional steps: • Ensure firewalls are configured to deny by default. • If a location is unmanned or if critical process data flows through a perimeter device, ensure redundancy exists or device failure won't prevent this data from being received by its intended destination. If the management environment is sufficiently isolated, then multifactor authentication may not be required to manage network devices. Adding multifactor requirements can limit the use of vendor supplied network monitoring solutions.

CIS Control 12 – Boundary Defense	
ICS Rationale, Applicability, and Considerations	
Introduction	This CIS Control focuses on the importance of managing the flow of information between networks of different trust levels. Alignment with the Purdue Reference Model[2] should be the primary goal when measuring the security architecture's effectiveness in an ICS network. When following this model, any ICS networks that require Internet connectivity should utilize a proxy. This proxy should not be dual-homed, nor perform as a bastion host, and it should reside within a less trusted, but still internal network (Level 4 or 5 from Purdue Model). This proxy device should be held to non-ICS security controls which may include the Sub-Controls not applicable to ICS networks. Note that a NAT or PAT firewall system is not a proxy and would not be considered an acceptable alternative.
Applicability	As stated above, ICS systems should not be directly connected to the internet. As such, any Sub-Controls referencing or inferring internet or web access are not applicable.
Considerations	For this CIS Control consider the following additional steps: • Ensure ICS and OT networks are not directly connected to the internet. • Maintain and enforce a minimum-security standard for all devices remotely logging into the organization's network. • Ensure systems with multiple network interfaces are not bridging (dual-homed) the OT network with any less trusted network. • Maintain logging of all activities and traffic that pass through this boundary, limiting services and clients to only those required to cross the security perimeter. • Recognize that not all traffic ingress or egress may necessarily pass through one device. For this reason, it is crucial to identify all known and potential means for crossing a secure perimeter, including rogue modems, wireless devices, cellular technologies, short-range wireless connections, etc. Consider collecting network analytical data (netflow, jflow, IPFix or similar). The idea here is to collect behavioral and analytical information rather than full packet captures. Limit access to trusted and necessary IP address ranges. Denying communication with known malicious or unused internet IP addresses is not necessary, as there should be no internet-web browsing capability from within the ICS. The list of internet addresses that need to be accessed should be very short, thus a whitelist style approach would be easier to implement and maintain. It is very common in ICS environments to utilize vendor or contractor remote access. Many times, these connections come from devices or systems owned by these third parties. When this is the case, it can be difficult to scan or utilize technical controls to enforce minimum security standards. Consider using non-technical controls such as signed agreements or reports generated by the third parties to ensure minimum security standards are maintained on the devices used to remotely connect. No ICS device or network should be visible from the Internet. However, certain efficiencies may be gained by passing information between an ICS network and less trusted (business) networks. Any device visible should reside in a DMZ. The Purdue Reference Model is a great resource for determining proper network architecture and determining if a network is less secure (resides at a higher layer).

[2] https://en.wikipedia.org/wiki/Purdue_Enterprise_Reference_Architecture
https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327

CIS Control 13 – Data Protection	
ICS Rationale, Applicability, and Considerations	
Introduction	This CIS Control's focus is on data protection and the relevance greatly varies based on ICS environment. These environments often do not contain much if any sensitive data in the traditional sense (PII, Credit Cards, etc.) In many ICS networks, control data consists of physical measurements such as flow, temperature, pressure, or valve readings and specific commands issued by logic control devices that control an overall process. This information is sometimes not deemed to be especially sensitive, or proprietary on its own and in some cases it is absent of any particular protections in the way it is collected, transferred, stored, and analyzed. However, some organizations consider this same information sensitive since it can indeed provide insights into an ICS design, connected products, proprietary process, production data, process variables, system schedules, configuration changes, and a bevy of other data that can provide significant intelligence to potential malefactors and wrong-doers. Some ICS environments there may be some information that is highly guarded and the ability to keep it confidential is key to the business success. This is often seen in the manufacturing space where recipes or formulas are used to make foods or chemicals. It is a growing concern for critical infrastructure ICS because it is recognized that such data leakage can aid an attacker in developing a strategy. What constitutes sensitive data is up to each OT team to assess. If it is concluded that no sensitive data is present, then this Control can be largely ignored. However, such a conclusion is expected to be a very rare exception.
Applicability	For ICS environments that do contain sensitive data, all the Sub-Controls are applicable.
Considerations	Sub-Controls related to automated and scheduled scanning might adversely affect the reliability of the system. Only scanning for sensitive data when it is safe to do so. Also, consider that encryption may not be feasible on all devices. For example, some embedded devices or network components may not be able to decrypt/encrypt data on removable media. Consider establishing a means to passively capture data from ICS using a variety of tools such as sniffers, protocol anomaly detection tools, and to periodically evaluate traffic streams for data leakage that could lead to misuse or abuse by a would-be attacker.

CIS Control 14 – Controlled Access Based on the Need to Know	
ICS Rationale, Applicability, and Considerations	
Introduction	The need to control access to systems based on the need to know is critically important. When following proper network layering (see the Purdue Reference Model), some degree of physical and logical segmentation will be in place. Devices that directly measure or control physical processes are typically segmented from general purpose workstations. However, segmentation within layers needs to also be considered. There are different approaches to network segmentation. For example, private VLANs are utilized heavily in IT and retail spaces. This approach may be applicable for ICS systems. However consideration needs to be given to ACLs to control access and other routing requirements when provisions for remote configuration and monitoring are requirements in highly segmented systems. Segmenting by subnets is typically an acceptable approach. VLANs or dedicated switches can be used depending on availability and cost requirements. There are many references to sensitive data through this Control. These references should align with the data protection control. This may remove applicability parts of this Control depending on ICS environment.
Applicability	Sub-Controls relating to private VLANs may not be applicable. Sub-Controls relating to sensitive information or data may not be applicable.
Considerations	In general, consider physical and logical network segmentation as a means to help ensure that authorized individuals and/or systems are restricted in how they communicate with other systems necessary to fulfill their specific responsibilities. However, segmentation via VLANS is not to be considered a security control because the complexity of managing VLAN routes, inter-VLAN routing, and susceptibility for network appliances including L3 switches and routers to be misconfigured or compromised will all affect the capability for VLAN to successfully restrict traffic. Physical network segmentation has greater capability to safeguard communications and operate as a mechanism of access control and isolate communications.

CIS Control 15 – Wireless Access Control	
ICS Rationale, Applicability, and Considerations	
Introduction	This CIS Control references the security of wireless access points. Networks with wireless access points can be accessed from outside the physical building where security controls may be present. Likewise, rogue access points can be used to gain unrestricted access to internal ICS networks. The presence and type of wireless networks vary depending on ICS vertical industry, application type, owner & operator requirements and desires, and even per laws and regulations when specialized wireless equipment is employed. Some OT teams use wireless where devices need to be mobile or when spread out. Another common scenario is wide area field mesh networks. Some teams relegate wireless to non-mission critical operations such as monitoring and diagnostics, or device and systems configuration. Some teams make broader use of wireless for even critical control operations, to connect to stranded assets, to improve device accessibility, to reduce costs, and to address limitations in available personnel, amongst other reasons.
Applicability	Sub-Controls related peer-to peer and untrusted device VLANs may not be applicable for this Control.
Considerations	For this CIS Control consider the following additional steps: • Strongly consider the ICS application and where wireless may be employed in mission critical aspects of operation that loss of communication, or a security breach may impact personal and functional safety, lead to ICS disruption, damage, or destruction of digital and physical products and services. • Ensure wireless ICS system utilizing Public Key Infrastructure (PKI), enforce expiration dates, non-repudiation and certificate chains validation, and revocation. • Ensure wireless (including cellular, sat, etc.) based ICS systems do not fail open when jammed. • Ensure wireless (including cellular, sat, etc.) based ICS networks are controlled/private networks. • Ensure software security patches and product upgrades are applied throughout the wireless infrastructure and products are kept current throughout their lifecycle. • Recognize that wired devices do have aspects of physical security that wireless devices may not similarly enjoy. This should lead to careful consideration of whether a device must necessarily be wireless, or if wired connection is more appropriate. • Where possible, limit wireless signal strength and range to what is necessary for the application in order to reduce the potential for remote accessibility of the connection from outside a security perimeter. References to wireless detection tools may not be applicable and should only alert on rogue devices connected to wireless access points. Profiling the device should only be done through passive means and denying device access should only be done where it won't impact the availability of the process. Use persistent, encrypted, defined point-to-point or point-to-multipoint wireless configuration. Both the base station and the remote station devices are specifically configured for secure communication. Do not permit or configure the system to allow ad hoc or guest connections.

CIS Control 15 – Wireless Access Control	
	Intrusion devices should also be limited to alerting unless denying a valid access point won't adversely impact the process. Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) or Elliptical Curve Cryptography (ECC) encryption with certificate based protection.

CIS Control 16 – Account Monitoring and Control	
ICS Rationale, Applicability, and Considerations	
Introduction	This CIS Control emphasizes the importance of controlling user access to systems in a typical network environment and ensuring effective account management. A common vulnerability can arise if employee accounts are not closed when employees leave the organization or change roles. ICS can be equally, if not more challenging because they often contain systems from different vendors, each with their own user account directories and often inconsistent set of individuals that may interact with a system. Additionally, remote and on-premises contractors and OEM technicians often request or require access either locally or remotely. These factors can make managing user accounts difficult for many OT teams, especially over a period of time given competing priorities for systems to be operating in a productive state, versus being idle for service and maintenance. While these factors can make user account control difficult, care must be taken not to inadvertently terminate or prevent a legitimate user from having the appropriate access as this might cause process disruption or delay. Furthermore, a balance must be considered and carefully managed between administrator-only account privileges versus group level privileges. Given the 24x7x365 operation of many ICS systems, incidents can occur at any time, including during a time when there is an absence of those with administrative privileges available to respond, remediate, and recover.
Applicability	Sub-Controls related to account expiration, inactivity lockouts, and multi-factor authentication are not applicable to ICS systems.
Considerations	For this CIS Control consider the following additional steps: • Used shared accounts and passwords only when necessary. • Establish and follow a process for changing shared account passwords immediately upon termination of any workforce member knowing the credentials. • Restrict shared operator account permissions to limit system access and changes. • Where possible, eliminate ICS applications leveraging clear text authentication or basic security authentication. Where not possible, use unique credential sets and monitor for their attempted usage elsewhere. • Consider access control chain-of-command plans for periods of time when normal personnel with required privileges may not be available. Consider monitoring the use of all accounts, automatically locking machines that are not used for process monitoring, or control after a standard period of inactivity. It is especially important to require the use of complex and long (14+) passwords or passphrases that are not easily guessed. Length over complexity makes current password cracking methods less effective and allows for users to more easily remember their passwords, reducing the chances of OT members not being able to log in, and the administrative overhead of resetting passwords.

CIS Control 16 – Account Monitoring and Control	
	In ICS environments, account access requirements are defined by job duties. Account access should be reviewed when personnel change roles, transfer, or are separated from the organization. Organizations should define a review schedule to verify that staff personnel are matched with the correct system access. Recommend at least annual reviews. • Establish a process for periodic privilege reviews to validate the necessary level of access, no less or no more than required, is in place for personnel and that said privileges match required duties, level of trust, and empowerment appropriate for said personnel.

CIS Control 17 – Implement a Security Awareness and Training Program	
ICS Rationale, Applicability, and Considerations	
Introduction	This CIS Control focuses on educating and training the typical enterprise workforce in a range of security practices that span basic to advanced skills to security awareness and vigilance. Human error, oversights, and negligence are leading causes of security weakness, and the consequences of untrained or inadequately, or infrequently trained personnel in an ICS environment and adjacent and interdependent systems can have a range of effects from disruption, damage to destruction of both a digital and physical nature. It is essential for OT teams to be thoroughly versed in security best practices so that they can ensure the security readiness of the ICS environment. These same skills should be nurtured and expanded over time to reinforce best practices and evolve as new risks are identified and new threats emerge. Additionally, many OT teams rely on contractors or vendors who need access to critical parts of the network to service specialized equipment, but they may not be aware of security threats. For these reasons, the experience and pedigree of these third-party resources should be carefully evaluated, including evaluation and validation of purported knowledge, skills, and abilities (KSAs) prior to allowing said third parties access to critical components and systems.
Applicability	Sub-Controls addressing the organizational workforce and testing employee awareness levels through phishing exercises are not applicable.
Considerations	For this CIS Control consider the following additional steps: • Implement a security awareness program that is mandated for completion by all visitors (Including 3rd parties: contractors, subcontractors, vendors, etc.) prior to granting remote or on-premises site access. • Consider awareness training that utilizes ICS relevant examples which are relevant to personnel interfacing with ICS. • Consider background checks and validation of credentials, experience, and certifications prior to third-party access to critical systems. • Consider baseline physical and cybersecurity security education to standardize knowledge, skills, and abilities (KSAs) for ICS personnel, as well as others that interface with and support ICS (e.g. IT personnel, IT-OT Hybrid personnel, third-party contractors, service/support personnel, and others as appropriate). • Consider advanced immersive cybersecurity security education and training for personnel expected to perform higher-risk, more advanced processes, or those who are making decisions relating to design, build, operation, and maintenance factors.

CIS Control 17 – Implement a Security Awareness and Training Program	
	• Consider standardizing on baseline and periodic measures of security KSAs including personnel capabilities assessments, required industry security certifications, security skills-building roadmaps to grow personnel capabilities over time to better safeguard systems, reinforce best practices, and evolve as new risks are identified and new threats emerge. When implementing security training, make sure the program also targets visitors and third-party contractors, vendors, or any outside party that will need access to internal ICS networks.

CIS Control 18 – Application Software Security	
ICS Rationale, Applicability, and Considerations	
Introduction	This Control focuses on the application security in the OT environment, where countless off-the-shelf, web-based, and proprietary applications can be running on a network. This can be a big task for system administrators. It is not uncommon for ICS environments to contain some custom-engineered, in-house built web-based, or other application software that is specialized for the given system. Such applications and services may not always follow a disciplined engineering development, test, and maintenance process. This can lead to application vulnerabilities that can be exploited by an attacker to aid in gaining access to or pivoting through ICS systems and network architectures. If an environment does contain this software, then this entire Control can be applied with minor modifications. This CIS Control is relevant to ICS environments if they contain web-based or other application software built by OT teams, and aspects of this Control even apply to commercial-off-the-shelf software sourced from product and solution vendors.
Applicability	All the Sub-Controls are applicable although Sub-Controls related to automated scanning may not be appropriate.
Considerations	In terms of firewalls, the goal is to protect the web applications when accessible from a lower security zone. Be sure to test in-house-developed and third-party-procured web applications for common security weaknesses using automated application scanners during scheduled maintenance when performance of these applications won't negatively affect the process. Monitoring for the release of software security patches and general product upgrades is an important aspect of maintaining software security. However, retesting after the application of said patches and upgrades is critical since it is not uncommon for new services, capabilities, features to be introduced or enabled, or configuration changes or resets to result from applying these patches and upgrades. Obtaining software patches and upgrades from only the most reputable sources and taking care in the secure transfer of these files is necessary to ensure software assurance, product, and system security. Verifying file hashes, or more ideally, making use of digitally signed software, and using only vendor-approved methods and tools to apply updates help with this assurance. Ensuring that the most current and relevant patch or software version is used, avoiding older versions that may contain known or unknown vulnerabilities also add to helping with software assurance.

CIS Control 18 – Application Software Security	
	For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested annually during scheduled maintenance. It is likely for OT teams to utilize scripts to perform routine tasks either locally or across a network. These tasks can be performing backup tasks, pruning old files, or capturing process data for historical tracking. When using scripts, it is important that they be written such that if an error occurs, the script will not continue to execute and cause undesired results. Often times, scripts require credentials to perform their intended operations. In these cases follow least-privilege practices and ensure technical controls are put into place to prevent unauthorized access to these credentials or scripts. Some examples of these technical controls are utilizing built-in scripting features to secure credentials (PowerShell secure-string) or applying controls from CIS Control 16.

CIS Control 19 – Incident Response and Management	
ICS Rationale, Applicability, and Considerations	
Introduction	This CIS Control addresses the processes and steps required to prepare for an incident. Well-defined and implemented incident response plans can allow an enterprise to identify, contain, reduce impacts, and more quickly recover from a cyber-incident. This is especially important for organizations where ICS downtime can lead to safety, health, or profitability impacts affecting the company, employees, customers, supply chain partners, community, and other constituents depending on the safe, reliable operation of an organization. Most OT teams are accustomed to performing some aspects of backups of critical systems to mitigate risks of failed components, loss of services, accidental employee actions, or even aspects of natural disasters. However, there is often a gap in the other areas of incident response, such as efficient coordination, chain of command, decision making authority, impact isolation, reporting, data collection, management responsibility, legal protocols, and communications strategy. Furthermore, it is not unusual for such processes to not be adequately or periodically tested, let alone evolve over time as new variables emerge, risks are identified, and threats evolve.
Applicability	All the Sub-Controls are applicable.
Considerations	For this CIS Control consider the following additional steps: • If extending an IT Incident Response plan, ensure the Incident Response Plan has been reviewed and approved by ICS Operational Leadership. • Response teams should be thoroughly familiar with the risks inherent to the ICS environment and mitigations to prevent secondary damage that may impact operational safety and protection of personnel, equipment, information, and a myriad of other dependent and interdependent factors. Aspects of this Control can mimic plans and procedures from non-ICS environments. However, it is not uncommon for these plans to require an augmentation of IT plans and procedures already in place for an enterprises Information technology systems in order to be relevant, applicable, and complete for OT.

CIS Control 20 – Penetration Tests and Red Team Exercises	
ICS Rationale, Applicability, and Considerations	
Introduction	This CIS Control is focused on designing and conducting controlled penetration testing in an operational technology environment, including connected devices and systems that may not be normally viewed as a constituent component, service, or system for an ICS. The goal is to test both employee responsiveness and the resiliency of internal controls. It refers to conducting tests on connected products, systems, and other interconnected products and systems in a real-time manner to identify, isolate, and demonstrate exploitability of a weakness or vulnerability in the security posture of the ICS. Processes controlled by ICS environments are easily disrupted by penetration testing, red team exercises, or other similar activity. Performing these activities on production systems, even during scheduled outages, can lead to downtime, destruction, injury, or introduce lingering artifacts that reduce the safety, efficiency, or performance of the tested system. For these reasons, it is highly recommended to only perform penetration testing and red-team exercises on non-production systems such as lab equipment, during scheduled-downtime, or during factory acceptance testing when proper oversights and precautions before a system is installed. However, such testing should be conducted periodically since system configurations change, new vulnerabilities are discovered, new threats emerge, and as tools and testing methodologies evolve. When analyzing production systems, it is recommended to use security assessments that are non-intrusive. These assessments can be paper based, utilize passive enumeration of system and network details, or any other activity that does not impact the safety, availability and performance of the ICS environment.
Applicability	Sub-Controls related to penetration tests or red team exercises on production systems do not apply. These Sub-Controls do apply when applied to testing on test bed or non-production systems.
Considerations	Instead of exclusively relying on an internal OT team, also consider conducting regular non-intrusive security assessments with the assistance of third-parties to identify a greater diversity of vulnerabilities and attack vectors that can be used to breach security of ICS systems. Ensure that personnel conducting vulnerability assessments are skilled in working within ICS environments to reduce the possibility of inadvertent negative impact to operations. Careful consideration should be given to the training, experience level, and pedigree of those performing such assessments. Include tests for the presence of unprotected system information, data leakage, and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, documents containing passwords, or other information critical to system operation. Consider using results from vulnerability scans and security assessments in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus security testing efforts. Furthermore, these results should operate as a guide for developing and applying corrective measures and other compensating controls to mitigate risks and better safeguard systems from threats. Personal and functional safety, as well as protecting digital and physical assets throughout the testing process is paramount. Testing an ICS environment's security

CIS Control 20 – Penetration Tests and Red Team Exercises	
	posture is important, but not as important as ensuring the safety of personnel and systems that are critical to continued operations.

Links and Resources

- **CIS Controls - https://www.cisecurity.org/controls/**
- **SANS Institute - https://www.sans.org/findtraining/**
- **ICS ISAC - http://ics-isac.org/blog/**
- **ICS Cert - https://ics-cert.us-cert.gov/**
- **ICS Security Resources and Tools - http://www.chemicalcybersecurity.org/RESOURCES-And-TOOLS**

In this document, we provide guidance on how to apply the security best practices found in CIS Controls Version 7[3] to ICS environments. As a non-profit driven by its volunteers, we are always in the process of looking for new topics and assistance in creating cybersecurity guidance. If you are interested in volunteering and/or have questions, comments, or have identified ways to improve this guide, please write us at controlsinfo@cisecurity.org.

All references to tools or other products in this document are provided for informational purposes only, and do not represent the endorsement by CIS of any particular company, product, or technology.

Contact Information
CIS
31 Tech Valley Drive
East Greenbush, NY 12061
518.266.3460
controlsinfo@cisecurity.org

[3] The newest version of the CIS Controls and other complementary documents may be found at www.cisecurity.org.