# Contents

# Cross-Sector Cybersecurity Performance Goals Controls List: Quick Guide

**CPG Expectations**

The CPGs are intended to be:

- A baseline set of cybersecurity practices broadly applicable across critical infrastructure with known risk-reduction value.
- A benchmark for critical infrastructure operators to measure and improve their cybersecurity maturity
- A combination of best practices for IT and OT owners, including a prioritized set of security controls.
- Unique from other control frameworks as they consider not only the practices that address risk to individual entities, but also the aggregate risk to the nation.

The CPGs are not:

- *Comprehensive:* The CPGs do not identify all the cybersecurity practices needed to protect national and economic security and public health and safety. They capture a core set of cybersecurity practices with known risk-reduction value broadly applicable across sectors.
- *Compulsory:* National Security Memorandum-5 does not create new authorities that compel owners and operators to adopt the CPGs or provide any reporting regarding or related to the CPGs to any government agency.

**CPG Guidelines**

- Mitigations must significantly reduce the risk/impact caused by well-known, probable threats and adversary tactics, techniques, and procedures (TTPs).
- Measurements must be clear, actionable, prescriptive easily attest-able, and concrete. Binary (yes/no) measurements are preferred.
- Avoid measurements that are scaled, such as “the number of devices with MFA enabled.”
- Good example(s):
    - “Establish minimum lengths for passwords, enforced by a system-wide policy on all IT and OT.” This example is clear, measurable (is there a system-wide minimum password policy or not), and not overly burdensome.
- Poor example(s):
    - “Implement Zero Trust.” While an important and valuable goal, ZT implementations are still poorly defined, hard to measure, and can be very burdensome for small organizations.

# 1.0 Account Security

| ID | Controls | Risk | Measurement | Scope | External References |
|---|---|---|---|---|---|
| 1.1 | Automatic account lockout after 5 or fewer failed login attempts should be enabled on all password protected IT and OT assets to reduce the risk of brute force attacks. This control should be verified by the implementation of system enforced policies to prevent login after a predetermined number of failed attempts. | | | | |
| | Automatic account lockout after failed login attempts | Brute force attacks<br>Password spraying | System-enforced policy that prevents future logins (for some minimum time, or until re-enabled by a privileged user) after 5 or fewer failed login attempts. This configuration should be enabled when available on an asset. | All password protected IT and OT assets, where technically capable | NIST CSF: PR.AC<br>ISA 62443-2-1 |
| 1.2 | Default passwords should be changed before installing or operationally deploying any IT or OT devices in order to reduce the risk of unauthorized credential access. This control should be verified by the implementation of a business process and policy that requires the changing of default passwords prior to being installed or placed in a production environment. | | | | |
| | Change default manufacturer passwords before installing or commissioning a device | Unauthorized access | An organization-wide, enforced policy that requires changing default manufacturer password for any/all devices before being commissioned and/or put on any production / internal network or the public internet. | All password protected IT and OT assets, where technically capable | NIST CSF: PR.AC<br>ISA 62443-2-1<br>ISA 62443-3-3 |
| 1.3 | A minimum password strength should be maintained on all IT and OT assets technically capable of sufficient password protection, in order to reduce the risk of credential access. This control should be verified through the implementation of system-enforced requirements for minimum password length, as well has a prohibition on the use of dictionary words. | | | | |
| | Minimum password strength | Brute force attacks<br>Password spraying | A system-enforced policy that mandates a minimum password length (generally 12 or more characters). | All password protected IT and OT assets, where technically capable | NIST CSF: PR.AC<br>ISA 62443-2-1<br>ISA 62443-3-3 |

| ID | Controls | Risk | Measurement | Scope | External References |
|---|---|---|---|---|---|
| 1.4 | Phishing resistant MFA should be implemented to reduce the risk of initial access and credential access attacks on. This control should be verified by the enrollment of all IT user accounts in MFA. For control systems assets, MFA should be enabled whenever possible, especially where remote access is being utilized, as well as all engineering workstations and HMIs. | | | | |
| | Phishing resistant MFA | Brute force attacks<br>Keylogging<br>Password spraying<br>Phishing | All accounts must leverage multi-factor authentication to access organizational resources.<br>- Hardware-based MFA when preferable, with soft tokens or other methods permissible when a hardware solution is not viable.<br>MFA must be enabled on:<br>- All accounts that access the OT network remotely<br>- All user and engineering workstations and<br>- All Human Machine Interface (HMIs) where technically capable | IT and OT assets | NIST CSF: PR.AC<br>ISA 62443-2-1<br>ISA 62443-3-3 |
| 1.5 | The principle of least privilege should be applied to all administrator or otherwise privileged accounts on both IT and OT, in order to reduce the risk of privilege escalation. This control should be measured by ensuring that the principle is being applied when granting privileges and confirming that no accounts are designated as domain administrators. | | | | |
| | Apply principle of least privilege to all administrator / privileged accounts | Privilege escalation<br>Unauthorized access | No user account should always have administrator or super-user privileges. | IT and OT assets | NIST CSF: PR.AC<br>ISA 62443-2-14.3.3.7.3<br>ISA 62443-3-3 1 |
| 1.6 | An organization should maintain unique credentials for a single user across similar services on IT and OT, in order to reduce the risk of initial access on both IT and OT assets. This control should be measured by confirming that IT and OT assets require unique credentials in order to access an account. | | | | |
| | Unique credentials between IT and OT networks | Unauthorized access | Credentials for similar services between the IT and OT networks must be different. | IT and OT assets | NIST CSF: PR.AC<br>ISA 62443-2-1 |

| ID | Controls | Risk | Measurement | Scope | External References |
|---|---|---|---|---|---|
| | | | | | ISA 62443-3-3 |

## 2.0 Device Security

| ID | Mitigation | Risk | Measurement | Scope | External References |
|---|---|---|---|---|---|
| 2.1 | Only approved hardware, firmware, and software may be installed on all (unless otherwise approved) IT and OT assets to reduce the risk of malware. This should be measured by the presence of enforce policy to require approval of any new software installation, and maintenance of an allow list of approved software. | | | | |
| | Only approved software can be installed on devices | Lateral movement | - An administrative policy that requires approval before (new) software is installed on a device<br>- Maintain an allow list of approved software | IT and OT assets | NIST CSF: DE.CM<br>ISA 62443-3-3:2013 |
| 2.2 | Applications running executable code (such as Microsoft macros or Open Office) should be disabled by default on all IT and OT assets to reduce the risk of malware. This control should be implemented by a policy to disable applications running executable code by default, and temporary exemptions must be justified per user and per device. | | | | |
| | Disable applications running executable code | Malware; Initial access | - A system-enforced policy on disables Microsoft Office macros by default on all user devices.<br>- If macros are necessary for organizational work, a process for requesting an authorized user to enable them *temporarily* | IT and OT assets | NIST CSF: PR.IP<br>ISA 62443-2-1<br>ISA 62443-3-3 |
| 2.3 | Owners/operators should maintain an accurate inventory of network connected assets to reduce the risk of unknown or improperly managed assets. This control should be verified by confirmation of a list of all assets with an IP address that is updated on a monthly basis. | | | | |
| | Inventory of network-connected hardware and software assets | Unknown assets<br>Un-/improperly managed assets (e.g., not patched, past end of life, etc.) | A regularly updated list of all organizational assets that have an IP address.<br>- Updated at least monthly | IT and OT assets | NIST CSF: ID.AM<br>ISA 62443-2-1<br>ISA 62443-3-3 |

| ID | Mitigation | Risk | Measurement | Scope | External References |
|---|---|---|---|---|---|
| 2.4 | Owner/operators should develop and maintain accurate documentation identifying baseline network topology and OT device configuration information to aid in both management and restoration activities. Cybersecurity managers must confirm the existence of this documentation, and institute a codified process to update this as necessary. | | | | |
| | Maintain current accurate documentation of infrastructure, to include baseline network topology, OT device configuration, etc. | Service continuity | - An accurate and maintained package of baseline documentation for all constituent components. | OT assets | NIST CSF: PR.IP<br>ISA 62443-2-1<br>ISA 62443-3-3 |

## 3.0 Data Security

| ID | Mitigation | Risks | Measurement | Scope | External References |
|---|---|---|---|---|---|
| 3.1 | Logs should be captured, stored, and protected to prevent data loss and aid in detection of malicious activity on both IT and OT systems. Organizations should verify that all access logs are securely stored and accessible only to privileged users. | | | | |
| | Logs applicable to security incidents and suspicious activity should be captured, stored, and protected. | Data Loss<br>Malware | - All access and security focused (e.g., IDS, firewall, DLP, VPN) logs are securely stored for potential use in future incident response or investigation.<br>- Logs may only be modified or deleted by privileged users<br>- Logs pertaining should only be available to privileged users to include security personnel. | IT and OT assets | NIST CSF: PR.PT<br>ISA 62443-2-1<br>ISA 62443-3-3 |
| 3.2 | All data, both in transit or at rest, should be encrypted to ensure confidentiality in both IT and CS. Owners/operators should verify that data is encrypted by a suitably strong algorithm. Additionally, any assets incapable of using suitable encryption should be prioritized for upgrade or replacement. | | | | |
| | Encrypt data in transit and at rest | Loss of data integrity<br>Loss of confidentiality | - All data in transit and at rest are encrypted by an appropriately strong algorithm<br>- No critical data should be stored in plain text.<br>- Utilization of transport layer security (TLS) to protect data in transit when technically feasible.<br>- Prioritize for upgrade or replacement of assets that do not support modern symmetric encryption (AES) | IT and OT assets | NIST CSF: PR.DS Data Security<br>ISA 62443-3-3 |

| ID | Mitigation | Risks | Measurement | Scope | External References |
|---|---|---|---|---|---|
| | | | - All passwords are salted and hashed. | | |

## 4.0 Governance & Training

| ID | Mitigation | Risk | Measurement | Scope | External References |
|---|---|---|---|---|---|
| 4.1 | Owners/operators should designate specific leaders as accountable parties for overseeing organizational IT and OT cybersecurity to ensure there is cybersecurity program accountability. This control can be executed by identifying a named individual who is responsible and accountable for cybersecurity. | | | | |
| | Entities must have designated leaders responsible for IT and OT cybersecurity | Program accountability<br>Lack of confidence in efficacy of controls execution | At least one person must be officially responsible and accountable for cybersecurity: handling incidents, developing plans, allocating budget. | IT and OT assets | NIST CSF: ID.GV Governance<br>ISA 62443-2-1 |
| 4.2 | As a subcomponent of an organizational cybersecurity program, owner/operators should designate an individual as the accountable party for the management of OT-specific cybersecurity concerns. | | | | |
| | Entities that own OT must ensure specially trained and qualified oversee cybersecurity of such assets. | Program accountability | - Named individual with official accountability and responsibility for planning, resourcing, and execution of OT cybersecurity activities.<br>- In small organizations this may be the same individual as identified in 4.1. | OT | NIST CSF: ID.GV<br>ISA 62443-2-1 |
| 4.3 | Owners/operators should provide basic cybersecurity training to all organizational employees and contractors to reduce the risk of both malicious and inadvertent threat activity. Reviewers should verify that all personnel receive training at least once annually. | | | | |
| | Security training | Initial Access<br>Defense Posture | - At least annual trainings for *all* organizational employees and contractors that | IT | NIST CSF: PR.AT Awareness and Training<br>ISA 62443-2-1 |

| ID | Mitigation | Risk | Measurement | Scope | External References |
|---|---|---|---|---|---|
| | | | covers basic security concepts, such as phishing, business email compromise, basic OPSEC, password security, etc.<br>- All new employees should receive initial cybersecurity training within 30 days of onboarding. | | |
| 4.4 | Owners/operators should provide OT/ICS-specific cybersecurity training to employees and contractors whose duties include utilization of OT/ICS to reduce the risk of both malicious and inadvertent insider threat activity. Reviewers should verify that all applicable personnel receive training at least once annually. | | | | |
| | OT/ICS-specific cybersecurity training | Initial Access<br>Defense Posture | - Ensure that personnel receive training tailored to their roles associated with OT/ICS.<br>- Training should be sourced from reputable ICS focused sources (e.g., CISA, SANS, ISA, etc. | OT | NIST CSF: PR.AT<br>ISA 62443-2-1 |

## 5.0 Vulnerability Management

| ID | Mitigation | Risk | Measurement | Scope | External References |
|---|---|---|---|---|---|
| 5.1 | Owner/operators should patch all Known Exploited Vulnerabilities in all public facing systems to reduce the risk of defense evasion by threat actors. Asset owners should validate that the KEV's listed at Known Exploited Vulnerabilities Catalog \| CISA are patched within the designated timeframe. When patching is not feasible, compensating controls should be applied and documented. | | | | |
| | Patch all Known Exploited Vulnerabilities (KEV) in public-facing systems | Defense evasion<br>Exploitation of known vulnerabilities to gain initial foothold | All KEV are patched or otherwise mitigated in public-facing systems within <X> timeframe of a vulnerability being published to the KEV list.<br>- Or, if impossible, implement an effective compensating control that makes exploiting that vulnerability impossible | All IT assets | NIST CSF: PR.IP ISA 62443-2-1 |
| 5.2 | Critical infrastructure organizations should establish a vulnerability disclosure program to reduce the risk of exploitation of vulnerabilities in their systems. Asset owners should confirm a method to receive and action publicly submitted vulnerabilities. | | | | |
| | Vulnerability Disclosure Program | Exploitable vulnerabilities<br>Vulnerable configurations | - A publicly accessible method, publicly listed and easily discoverable, for security researchers to submit vulnerabilities and otherwise contact security staff (such as a web portal or email address)<br>- Submissions must be acknowledged and responded to in a timely manner.<br>- If and when vulnerabilities are validated and disclosed, public acknowledgement is given to the researcher who originally submitted the vulnerability. | IT and OT assets | NIST CSF: RS.AN |
| 5.3 | Owner/operators should ensure that there are no exploitable ports directly exposed to public internet facing assets to reduce the probability of threat initial access via public internet. | | | | |

| ID | Mitigation | Risk | Measurement | Scope | External References |
|---|---|---|---|---|---|
| | No exploitable exposed ports & services on public-facing assets (e.g., RDP) | Initial access | - No exploitable exposed ports & services on public-facing assets (e.g., RDP) | IT and OT assets | NIST CSF: PR.PT<br>ISA 62443-2-1 |
| 5.4 | Owner/operators should ensure that no ICS is connected to the public internet unless explicitly required for operation. Organizations should verify that for any internet connected ICS asset, there is a documented justification. | | | | |
| | ICS should not be connected to internet unless explicitly required for operations | Initial access | - Organizations must have a justification for all OT devices that are on the public internet<br>- All internet-facing OT systems possess multi-factor authentication for access, other compensating controls, and have network traffic logged | OT assets | NIST CSF: PR.PT<br>ISA 62443-2-1 |
| 5.5 | Owner/operators should conduct adversary emulation (e.g., red team and/or purple team) testing on an annual basis to identify vulnerabilities across all IT and OT assets, and remediate any identified issues as soon as possible. Organizations should confirm that they conduct such tests on a recurring basis not to exceed 24 months between exercises, and that identified vulnerabilities are addressed in manner so as to be confirmed as resolved future testing. | | | | |
| | Regular adversary emulation testing and mitigation of high-impact findings | Initial Access<br>Reconnaissance<br>Adversary persistence<br>Operational impact | - Adversary emulation exercises are conducted at least annually by a qualified team with demonstrated experience in testing OT/ICS cybersecurity.<br>- These exercises, which may include penetration tests or bug bounties, should include both unannounced and announced tests.<br>- These exercises should test the ability for a sophisticated adversary to infiltrate the network from the outside, as well as the ability of an adversary within the network (e.g., | IT and OT assets | NIST CSF: RS.IM<br>ISA 62443-2-1 |

| ID | Mitigation | Risk | Measurement | Scope | External References |
|---|---|---|---|---|---|
| | | | "assume breach") to pivot laterally to demonstrate potential impact on OT/ICS systems.<br>- Evidence that high-impact findings from previous tests are mitigated in a timely manner and aren't re-observed in the following test | | |

## 6.0 Supply Chain / Third Party

| ID | Mitigation | Risk | Measurement | Scope | External References |
|---|---|---|---|---|---|
| 6.1 | Owner/operators should include security capability as evaluation criteria for the procurement of IT and OT assets or services to reduce the risk of deploying assets that are not secure by design and are not future-proofed. Organizations should verify that such requirements are captured in RFI's/RFQ's and contractually enforced. | | | | |
| | Procurement evaluations | Procuring assets and services unable to be adequately secured in the context of their intended use | - Language in procurement documents that, given two roughly equivalent products or services in terms of function or cost, the one that demonstrates a stronger security posture will be evaluated higher. | All IT and OT assets and services | NIST CSF: ID.SC<br>ISA 62443-2-1 |
| 6.2 | Owner/operators should require that all IT or OT vendors or service providers notify them of any security incidents or breaches in a reasonable timeframe to reduce the risk of threat actor exploitation. Organizations should include contract clauses in all procurements or SLA's stipulating said notification. | | | | |
| | Requiring vendors/providers to notify customers of potential incidents | Exploitation<br>Initial Access<br>Data loss | Do procurement documents and contracts necessitate that vendors/providers notify customers of potential security incidents within a reasonable timeframe? | All IT and OT assets or services | NIST CSF: ID.SC<br>ISA 62443-2-1 4.3.2.6.7<br>ISA 62443-3-3 |
| 6.3 | Owner/operators should require that all IT or OT vendors or service providers notify them of any security vulnerabilities in a reasonable timeframe to reduce the risk of threat actor exploitation. Organizations should include contract clauses in all procurements or SLA's stipulating said notification. | | | | |
| | Requiring vendors/providers to notify customers of vulnerabilities in their products, services, etc. | Exploitation<br>Initial Access<br>Data loss | Do procurement documents and contracts necessitate that vendors/providers notify customers of potential | All IT and OT assets or services | NIST CSF: ID.SC<br>ISA 62443-2-1<br>ISA 62443-3-3 |

| ID | Mitigation | Risk | Measurement | Scope | External References |
|---|---|---|---|---|---|
| | | | security vulnerabilities within a reasonable timeframe? | | |

## 7.0 Resilience

| ID | Mitigation | Risk | Measurement | Scope | CSF Category |
|---|---|---|---|---|---|
| 7.1 | Owners/operators should report cybersecurity incidents across IT and OT assets to CISA, as well as any other mandatory reporting stakeholders for each organization, as soon as possible to minimize the impact of threat activity internally and enhance community ability to position to meet emerging or active threats. The control shall be validated by the presence of codified policy and defined procedure on how and to whom to report incidents. | | | | |
| | Report all and potential cybersecurity incidents to internal stakeholders and external groups (e.g., CISA, SRMA, and/or ISAC) | Malicious activity | - Codified policy to and procedures on to whom and how to report all (confirmed and potential) cybersecurity incidents to external entities<br>- Confirmed or suspected incidents should be reported within 96 hours. | IT and OT assets | NIST CSF: RS.CO<br>ISA 62443-2-1 |
| 7.2 | Owner/operators should develop, maintain, and practice incident response plans to ensure effective response to threat actions against all assets. Organizations should validate existing Incident Response (IR) plans at a minimum with tabletop exercises or reviews of actual incident responses on a regularly recurring basis (e.g., biennially). | | | | |
| | Entities must have and regularly drill & update IR plans | Prolonged and/or insufficiently remediated incident response | IR plans for common threat scenarios and any scenarios specifically relevant for the organization exist and are regularly updated and drilled. | IT and OT assets | NIST CSF: PR.IP<br>ISA 62443-2-1 |
| 7.3 | Critical IT or OT systems should be backed up and tested on a regular basis and stored in a secure manner, in order to mitigate the risk of disruption of operations and data loss. | | | | |
| | Critical systems should be regularly backed up, and the backups should be tested and protected. | Disruption of operations<br>Data loss | - All systems that are necessary for operations are regularly backed up. | IT and OT assets | NIST CSF: PR.IP<br>ISA 62443-2-1<br>ISA 62443-3-3 |

| ID | Mitigation | Risk | Measurement | Scope | CSF Category |
|---|---|---|---|---|---|
| | | | - These backups are stored separately from the source systems and are regularly tested.<br>- Stored information should include at a minimum; configurations, roles, PLC logic, and engineering drawings. | | |
| 7.4 | Owners/operators should develop, implement, maintain, and test control systems response and recovery plans to limit the risk of impact of any cyberattack and minimize disruption to service. | | | | |
| | Implement and test control system response and recovery plans with clearly defined roles and responsibilities. | Disruptions to delivery of services. | - Develop control system cybersecurity response and recovery plans. These plans should have clearly defined roles, and be tested on a regular basis to ensure effectiveness in ensuring continuity of critical functions.<br>- Recovery plans developed, maintained, and tested from a full stop (Dark Start) every 12 months. | OT | NIST CSF: PR:IP<br>ISA 62443-2-1<br>ISA 62443-3-3 |

## 8.0 Network Segmentation

| ID | Mitigation | Risk | Measurement | Scope | External References |
|---|---|---|---|---|---|
| 8.1 | Owners/operators should limit the connections between IT and OT to the greatest extent possible to reduce the risk of threat initial access via pivot from IT to OT. Organizations should verify that all OT/IT connections are logged and monitored for suspicious activity or unauthorized access. | | | | |
| | Connections between IT and OT should be restricted and monitored. | Initial access | - All connections between the OT an IT networks (including via a DMZ or similar intermediary) are logged, and users are notified of unauthorized or suspicious connections.<br>- All connections to the OT network should be denied by default unless explicitly allowed (e.g., by IP address and port) for specific system functionality. | IT and OT assets | NIST CSF: PR.AC<br>ISA 62443-2-1<br>ISA 62443-3-3 |
| 8.2 | All owner/operators should implement segmentation between IT and OT networks to prevent initial access by threat actors. Organizations should verify that devices on either side of segmentation lines/safety zones must not connect to the opposite side with minimal exceptions and only through a correctly configured firewall or comparable alternative. | | | | |
| | Segment IT/OT networks | Lateral movement (OT network compromise from IT network) | - A device on either side of the OT/IT segmentation should not be able to connect to the other side unless explicitly allowed. | IT and OT assets | NIST CSF: PR.AC<br>ISA 62443-2-1<br>ISA 62443-3-3 |

| ID | Mitigation | Risk | Measurement | Scope | External References |
|---|---|---|---|---|---|
| | | | - Communications into the OT network must go through a tightly controlled and logged intermediary, such as a bastion host or a “jump box.” | | |

## 9.0 Physical Security

| ID | Mitigation | RISK | Measurement | Scope | External References |
|---|---|---|---|---|---|
| 9.1 | Owners/operators should limit physical access to control systems and related IT equipment to only authorized personnel to prevent initial access by threat actors. Organizations should confirm that all HMI's and other hardware are secured behind locked gating with monitored and logged access logs. | | | | |
| | Restrict physical access to control systems and connected equipment to authorized personnel with a need for access | Unauthorized access | Only authorized personnel can access control systems, especially to human machine interfaces and engineering workstations. | All OT and related IT infrastructure | NIST CSF: PR.AC<br>ISA 62443-2-1 |
| 9.2 | Owners/operators should ensure that unauthorized media and hardware are never connected to OT infrastructure and related IT infrastructure to prevent the use of such mediums as a vector for malware and threat actor initial access. Organizations should disable or remove physical access ports, as well as establish procedures for granting access on a by exception basis. | | | | |
| | Ensure that unauthorized portable media devices and other hardware are unable to be connected to control systems | Malware<br>Initial Access | - Organization has an established policy and process to ensure that only controlled, scanned, and authorized and verified devices should be allowed to connect to OT assets.<br>- Organization has procedures to remove, disable, or otherwise secure physical ports to prevent the<br>- connection of unauthorized devices<br>- | All OT and related IT infrastructure | NIST CSF: PR.PT<br>ISA 62443-3-3 |
| 9.3 | Owners/operators should define which utilities are essential to maintain operations (such as water, power, and HVAC), and deploy and regularly test failover systems to ensure uninterrupted supply of these resources. | | | | |
| | Establish environmental controls to maintain temperature and other | Physical/environmental damage | Organization maintains failover systems or other secondary systems (e.g. backup power) to | All OT and related IT infrastructure | NIST CSF: PR.IP |

| ID | Mitigation | RISK | Measurement | Scope | External References |
|---|---|---|---|---|---|
| | physical factors that can damage sensitive equipment | | maintain physical stasis in the event of an outage | | ISA 62443-2-1 |