

D.1 Mapping NIST Cybersecurity Framework v2.0 subcategories to Cyber/Physical Security Framework v1.1

NIST Cyberseucurity Framework Ver 2.0			Cyber/Physical Security Framework Ver 1.1	
Function	Subcategory-ID	Subcategory	Measure Requirement ID	Measure Requirement
Govern (GV)	GV.OC-01	The organizational mission is understood and informs cybersecurity risk management	CPS.GV.OC-01	The organization understands its mission and uses it to inform cybersecurity risk management decisions.
	GV.OC-02	Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	CPS.GV.SC-04	The organization identifies and prioritizes organizations and people that play an important role relevant in each layer of the three-layer structure to sustain business operations.
	GV.OC-03	Legal, regulatory, and contractual requirements regarding cybersecurity - including privacy and civil liberties obligations - are understood and managed	CPS.GV.OC-02	The organization understands legal, regulatory, and contractual requirements regarding cybersecurity—including privacy and civil liberties obligations—as well as industry guidelines, and establishes internal rules that appropriately reflect and address these requirements or guidelines.
	GV.OC-04	Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated	CPS.GV.OC-03	The organization identifies dependencies and critical functions across both its own organization and related external entities to sustain business operations and shares them with those external entities.
	GV.OC-05	Outcomes, capabilities, and services that the organization depends on are understood and communicated	CPS.GV.OC-03	The organization identifies dependencies and critical functions across both its own organization and related external entities to sustain business operations and shares them with those external entities.
	GV.RM-01	Risk management objectives are established and agreed to by organizational stakeholders	CPS.GV.RM-01	The organization defines risk management objectives and agrees on them with relevant stakeholders.
	GV.RM-02	Risk appetite and risk tolerance statements are established, communicated, and maintained	CPS.GV.RM-03	The organization establishes its risk appetite and risk tolerance, and communicates them across the organization.
	GV.RM-03	Cybersecurity risk management activities and outcomes are included in enterprise risk management processes	CPS.GV.RM-04	The organization integrates cybersecurity risk management activities and their outcomes into the organizational risk management process, managing cybersecurity risks within that process.
	GV.RM-04	Strategic direction that describes appropriate risk response options is established and communicated	CPS.GV.RM-05	The organization formulates policies regarding risk response options and their operations, and shares them within the organization.
	GV.RM-05	Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	CPS.GV.RM-06	The organization establishes and maintains lines of communication across the organization regarding cybersecurity risks, including risks posed by partners and other third parties.
	GV.RM-06	A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	CPS.GV.RM-07	The organization standardizes methodologies for assessing, documenting, classifying, and prioritizing cybersecurity risks, and shares them within the organization.
	GV.RM-07	Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions	CPS.GV.RM-08	The organization identifies strategic opportunities (positive risks for the organization), clarifies their characteristics, and integrates them into organizational cybersecurity risk deliberations.
	GV.RR-01	Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving	CPS.GV.RR-01	Organizational senior management is responsible and accountable for cybersecurity risk, fostering a culture that is risk-aware, ethical, and continually improving.
	GV.RR-02	Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	CPS.GV.RR-02	The organization establishes roles, responsibilities, and authorities related to its cybersecurity risk management and communicates them within the organization.
	GV.RR-03	Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies	CPS.GV.RR-04	The organization allocates necessary resources commensurate with its cybersecurity strategy, roles, responsibilities, and policies.
	GV.RR-04	Cybersecurity is included in human resources practices	CPS.GV.RR-05	The organization incorporates security-related matters (e.g., revoking access privileges and screening employees) into measures that address role changes resulting from personnel transfers.
	GV.PO-01	Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	CPS.GV.PO-01	The organization formulates security policies based on its organizational context, cybersecurity strategy, and priorities, communicates them within the organization and to relevant external parties (including suppliers and third-party providers, as needed), and implements them.
	GV.PO-02	Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission	CPS.GV.PO-02	The organization periodically reviews its security policies and updates them as necessary, based on changes in requirements, threats, technology, and the organization’s mission.
	GV.OV-01	Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction	CPS.GV.OV-01	The organization reviews the outcomes of its cybersecurity strategy and, taking into account these results and changes in the internal and external context, revises the cybersecurity strategy as well as enterprise-wide strategy and direction as necessary.
	GV.OV-02	The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks	CPS.GV.OV-01	The organization reviews the outcomes of its cybersecurity strategy and, taking into account these results and changes in the internal and external context, revises the cybersecurity strategy as well as enterprise-wide strategy and direction as necessary.
	GV.OV-03	Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed	CPS.GV.OV-02	The organization reviews the implementation status of its cybersecurity risk management and updates it as necessary.

Appendix D.1 - Mapping NIST CSF Ver 2.0 to CPSF Ver 1.1

NIST Cyberseucurity Framework Ver 2.0			Cyber/Physical Security Framework Ver 1.1	
Function	Subcategory-ID	Subcategory	Measure Requirement ID	Measure Requirement
	GV.SC-01	A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders	CPS.GV.SC-01	The organization establishes supply chain risk management programs, strategies, objectives, policies, and processes, and operates them upon agreement with organizational stakeholders.
	GV.SC-02	Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally	CPS.GV.SC-02	The organization establishes cybersecurity roles and responsibilities for suppliers and partners, communicates them internally and externally, and coordinates adjustments as necessary.
	GV.SC-03	Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes	CPS.GV.SC-03	The organization integrates cybersecurity supply chain risk management into its cybersecurity and enterprise risk management, risk assessment, and improvement processes.
	GV.SC-04	Suppliers are known and prioritized by criticality	CPS.GV.SC-04	The organization identifies and prioritizes organizations and people that play an important role relevant in each layer of the three-layer structure to sustain business operations.
	GV.SC-05	Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties	CPS.GV.SC-05	The organization establishes supply chain cybersecurity standards considering the lifecycle of business relationships, clearly defines the scope of responsibilities, and agrees on them with partners through contracts or other means.
	GV.SC-06	Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships	CPS.GV.SC-06	Before concluding contracts with suppliers and other third parties, the organization evaluates the cybersecurity management posture of said suppliers and third parties, and takes necessary measures to mitigate risks as needed.
	GV.SC-07	The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship	CPS.GV.SC-04	The organization identifies and prioritizes organizations and people that play an important role relevant in each layer of the three-layer structure to sustain business operations.
			CPS.GV.SC-06	Before concluding contracts with suppliers and other third parties, the organization evaluates the cybersecurity management posture of said suppliers and third parties, and takes necessary measures to mitigate risks as needed.
			CPS.GV.SC-07	When entering into contracts with other relevant organizations such as business partners, the organization considers its objectives and risk management outcomes, verifying that products and services provided by them conform to the organization's security requirements.
			CPS.GV.SC-08	The organization periodically evaluates other relevant organizations such as business partners using audits, test results, or other forms of assessment to confirm that they are fulfilling their contractual obligations.
			CPS.GV.SC-09	The organization establishes and implements procedures to be followed when non-compliance with contractual requirements is identified through audits or testing of other relevant organizations such as business partners.
			CPS.GV.SC-10	The organization establishes policies and procedures for determining, based on the criticality of the technology products and services to be procured, those for which records of their sources and, to the extent reasonably ascertainable, their distribution channels are to be obtained.
	GV.SC-08	Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	CPS.RS.MA-01	To clarify response actions, priorities, and remediation scope following the occurrence of a security incident, the organization predefines and implements response procedures (security operation processes) for the organization, people, components, and systems after detecting an incident.
			CPS.RS.MA-04	Once a security incident is declared, the organization executes incident response in accordance with predefined procedures, coordinating with other relevant organizations such as business partners.
			CPS.RC.CO-01	The organization establishes and maintains rules regarding information exchange aimed at recovery after the occurrence of a security incident.
	GV.SC-09	Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle	CPS.GV.SC-03	The organization integrates cybersecurity supply chain risk management into its cybersecurity and enterprise risk management, risk assessment, and improvement processes.
			CPS.GV.SC-10	The organization establishes policies and procedures for determining, based on the criticality of the technology products and services to be procured, those for which records of their sources and, to the extent reasonably ascertainable, their distribution channels are to be obtained.
	GV.SC-10	Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement	CPS.GV.SC-08	The organization periodically evaluates other relevant organizations such as business partners using audits, test results, or other forms of assessment to confirm that they are fulfilling their contractual obligations.
			CPS.GV.SC-09	The organization establishes and implements procedures to be followed when non-compliance with contractual requirements is identified through audits or testing of other relevant organizations such as business partners.
			CPS.GV.SC-10	The organization establishes policies and procedures for determining, based on the criticality of the technology products and services to be procured, those for which records of their sources and, to the extent reasonably ascertainable, their distribution channels are to be obtained.
			CPS.GV.SC-11	The organization establishes and implements procedures to be followed upon the termination of contracts with partners and other parties.

Appendix D.1 - Mapping NIST CSF Ver 2.0 to CPSF Ver 1.1

NIST Cyberseucurity Framework Ver 2.0			Cyber/Physical Security Framework Ver 1.1	
Function	Subcategory-ID	Subcategory	Measure Requirement ID	Measure Requirement
Identify (ID)	ID.AM-01	Inventories of hardware managed by the organization are maintained	CPS.ID.AM-01	The organization develops and appropriately manages inventories of hardware, software, and their management information (e.g., name, version, network address, designated manager, and license information) that comprise its system.
	ID.AM-02	Inventories of software, services, and systems managed by the organization are maintained	CPS.ID.AM-01	The organization develops and appropriately manages inventories of hardware, software, and their management information (e.g., name, version, network address, designated manager, and license information) that comprise its system.
	ID.AM-03	Representations of the organization's authorized network communication and internal and external network data flows are maintained	CPS.ID.AM-02	The organization develops and appropriately manages communication network diagrams and data flow diagrams within the organization.
	ID.AM-04	Inventories of services provided by suppliers are maintained	CPS.ID.AM-03	The organization develops and appropriately manages inventories of external information systems connected to its organizational assets.
	ID.AM-05	Assets are prioritized based on classification, criticality, resources, and impact on the mission	CPS.ID.AM-04	The organization categorizes and prioritizes resources (e.g., components, data, and systems) based on their function, criticality, and business value, defines management responsibilities, and communicates them to relevant organizations and people involved in their operation.
	ID.AM-07	Inventories of data and corresponding metadata for designated data types are maintained	CPS.ID.AM-05	The organization develops and appropriately manages inventories of data and metadata in its possession.
	ID.AM-08	Systems, hardware, software, services, and data are managed throughout their life cycles	CPS.ID.AM-06	The organization manages systems, hardware, software, services, and data throughout their entire lifecycle, from acquisition to disposal.
	ID.RA-01	Vulnerabilities in assets are identified, validated, and recorded	CPS.ID.RA-01	The organization identifies vulnerabilities in its assets and manages them by linking them to the corresponding assets.
	ID.RA-02	Cyber threat intelligence is received from information sharing forums and sources	CPS.ID.RA-02	The organization establishes a process to collect, analyze, respond to, and utilize vulnerability and threat information from internal and external sources (e.g., internal tests, security information, and security researchers).
	ID.RA-03	Internal and external threats to the organization are identified and recorded	CPS.ID.RA-03	- The organization identifies and documents potential security incidents, their impacts, and their causal factors regarding organizational assets. - From the planning and design stages of IoT devices and IoT-integrated systems, the organization verifies that no unacceptable known security risks exist, incorporating safety hazard perspectives.
	ID.RA-04	Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	CPS.ID.RA-04	The organization identifies the potential impact and likelihood of threats exploiting vulnerabilities by periodically conducting risk assessments to evaluate the effectiveness of security rules for component management, including their implementation methods.
	ID.RA-05	Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization	CPS.ID.RA-04	The organization identifies the potential impact and likelihood of threats exploiting vulnerabilities by periodically conducting risk assessments to evaluate the effectiveness of security rules for component management, including their implementation methods.
	ID.RA-06	Risk responses are chosen, prioritized, planned, tracked, and communicated	CPS.ID.RA-06	- Based on risk assessments, the organization clearly defines response measures for potential security risks, documents the defined scope and priorities of response actions, monitors the implementation progress, and communicates this status to relevant parties. - The organization appropriately addresses security and associated safety risks identified through the assessment in the planning and design stages of IoT devices and IoT-integrated systems.
	ID.RA-07	Changes and exceptions are managed, assessed for risk impact, recorded, and tracked	CPS.ID.RA-07	The organization assesses the risk impact posed by significant organizational changes and security requirement exceptions, and records and manages the results.
	ID.RA-08	Processes for receiving, analyzing, and responding to vulnerability disclosures are established	CPS.ID.RA-02	The organization establishes a process to collect, analyze, respond to, and utilize vulnerability and threat information from internal and external sources (e.g., internal tests, security information, and security researchers).
	ID.RA-09	The authenticity and integrity of hardware and software are assessed prior to acquisition and use	CPS.PR.PS-01	The organization evaluates the authenticity and integrity of hardware and software prior to acquisition and deployment, and verifies their integrity during operation.
	ID.RA-10	Critical suppliers are assessed prior to acquisition	CPS.GV.SC-04	The organization identifies and prioritizes organizations and people that play an important role relevant in each layer of the three-layer structure to sustain business operations.
	ID.IM-01	Improvements are identified from evaluations	CPS.ID.IM-01	The organization continuously improves its cybersecurity management posture under normal and adverse conditions, including the perspectives outlined in CPS.ID.IM-02 and subsequent requirements.
	ID.IM-02	Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties	CPS.ID.IM-01	The organization continuously improves its cybersecurity management posture under normal and adverse conditions, including the perspectives outlined in CPS.ID.IM-02 and subsequent requirements.
			CPS.ID.IM-03	The organization continuously improves security training and education programs for its personnel and designated contacts at critical partner organizations.
	ID.IM-03	Improvements are identified from execution of operational processes, procedures, and activities	CPS.ID.IM-01	The organization continuously improves its cybersecurity management posture under normal and adverse conditions, including the perspectives outlined in CPS.ID.IM-02 and subsequent requirements.
	ID.IM-04	Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	CPS.ID.IM-06	The organization incorporates lessons learned from responses to security incidents to continuously improve its incident response plan.
			CPS.RS.MA-01	To clarify response actions, priorities, and remediation scope following the occurrence of a security incident, the organization predefines and implements response procedures (security operation processes) for the organization, people, components, and systems after detecting an incident.

Appendix D.1 - Mapping NIST CSF Ver 2.0 to CPSF Ver 1.1

NIST Cyberseucurity Framework Ver 2.0			Cyber/Physical Security Framework Ver 1.1	
Function	Subcategory-ID	Subcategory	Measure Requirement ID	Measure Requirement
Protect (PR)	PR.AA-01	Identities and credentials for authorized users, services, and hardware are managed by the organization	CPS.PR.AA-01	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.
	PR.AA-02	Identities are proofed and bound to credentials based on the context of interactions	CPS.PR.AA-02	The organization authenticates and authorizes logical access to components (physical items, systems, etc.) by IoT devices and users using highly reliable methods (e.g., multi-factor authentication) commensurate with transaction risks (personal security, privacy risks, and other organizational risks).
	PR.AA-03	Users, services, and hardware are authenticated	CPS.PR.AA-02	The organization authenticates and authorizes logical access to components (physical items, systems, etc.) by IoT devices and users using highly reliable methods (e.g., multi-factor authentication) commensurate with transaction risks (personal security, privacy risks, and other organizational risks).
	PR.AA-04	Identity assertions are protected, conveyed, and verified	CPS.PR.AA-04	The organization protects, transmits, receives, and verifies information regarding authenticated entities (ID assertions).
	PR.AA-05	Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	CPS.PR.AA-05	The organization defines rules regarding the granting of access privileges in its security policies and incorporates the principles of least privilege and separation of duties.
			CPS.PR.AA-06	The organization periodically reviews granted access privileges and remediates unnecessary or excessive permissions.
	PR.AA-06	Physical access to assets is managed, monitored, and enforced commensurate with risk	CPS.PR.AA-07	The organization implements physical safeguards, such as locking installation areas for IoT devices, servers, and related assets, controlling entry and exit, deploying biometric authentication, installing surveillance cameras, and conducting baggage and weight inspections.
	PR.AT-01	Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind	CPS.PR.AT-01	The organization conducts appropriate training and education for all personnel to carry out their assigned roles and responsibilities to minimize the occurrence and impact of security incidents, and maintains records of such activities.
	PR.AT-02	Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind	CPS.PR.AT-01	The organization conducts appropriate training and education for all personnel to carry out their assigned roles and responsibilities to minimize the occurrence and impact of security incidents, and maintains records of such activities.
			CPS.PR.AT-02	The organization provides appropriate training and security education to designated personnel of external partners critical to security management, who may be involved in security incident response for the organization, enabling them to fulfill their assigned roles, and maintains records of such activities.
	PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected	CPS.PR.DS-02	The organization protects the confidentiality, integrity, and availability of data-at-rest.
	PR.DS-02	The confidentiality, integrity, and availability of data-in-transit are protected	CPS.PR.DS-03	The organization protects the confidentiality, integrity, and availability of data-in-transit.
	PR.DS-10	The confidentiality, integrity, and availability of data-in-use are protected	CPS.PR.DS-04	The organization protects the confidentiality, integrity, and availability of data-in-use.
	PR.DS-11	Backups of data are created, protected, maintained, and tested	CPS.PR.DS-06	The organization performs routine backups of data (e.g., component configurations and operational data), protects backup data, and tests restoration capabilities.
	PR.PS-01	Configuration management practices are established and applied	CPS.PR.PS-06	The organization establishes and applies configuration management practices for hardware and software of IoT devices, servers, and related assets (including minimizing functionality by physically or logically disabling unnecessary network, USB, and serial ports).
	PR.PS-02	Software is maintained, replaced, and removed commensurate with risk	CPS.ID.AM-06	The organization manages systems, hardware, software, services, and data throughout their entire lifecycle, from acquisition to disposal.
			CPS.PR.PS-09	The organization applies security-critical updates for IoT devices, servers, and related assets in a timely manner using managed tools while appropriately recording history.
	PR.PS-03	Hardware is maintained, replaced, and removed commensurate with risk	CPS.ID.AM-06	The organization manages systems, hardware, software, services, and data throughout their entire lifecycle, from acquisition to disposal.
			CPS.PR.PS-12	Upon the disposal of IoT devices, servers, and related assets, the organization deletes or renders unreadable all internally stored data, unique identifiers of legitimate devices and systems, and critical security information (e.g., private keys and digital certificates).
	PR.PS-04	Log records are generated and made available for continuous monitoring	CPS.PR.PS-11	To appropriately detect security incidents, the organization determines and documents the scope and types of events for audit logging, and continuously records and reviews logs.
	PR.PS-05	Installation and execution of unauthorized software are prevented	CPS.PR.PS-07	The organization prevents the installation and execution of unauthorized software.
	PR.PS-06	Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle	CPS.PR.PS-05	The organization integrates secure software development practices (e.g., security reviews during the design stage, application of secure coding rules, and pre-release vulnerability assessments) into the system development life cycle and verifies their implementation.
	PR.IR-01	Networks and environments are protected from unauthorized logical access and usage	CPS.PR.IR-01	The organization protects networks and environments from unauthorized access and use by implementing network segmentation (e.g., separating development/test environments from production environments, and isolating IoT device environments from other networks within the organization).
	PR.IR-02	The organization's technology assets are protected from environmental threats	CPS.PR.IR-02	The organization implements physical safeguards to comply with policies and rules regarding the physical operating environment of its IoT devices, servers, and related assets, such as ensuring uninterruptible power supplies, fire protection equipment, and flood protection measures.
	PR.IR-03	Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	CPS.PR.IR-03	The organization implements mechanisms to achieve requirements for the continuous operation of systems and services under normal and adverse conditions.
	PR.IR-04	Adequate resource capacity to ensure availability is maintained	CPS.PR.IR-04	The organization secures sufficient resources (e.g., people, components, and systems) to minimize the impact of attacks and maintain critical functions, even in the event of cyberattacks such as ransomware or denial-of-service (DoS) attacks.

Appendix D.1 - Mapping NIST CSF Ver 2.0 to CPSF Ver 1.1

NIST Cyberseucurity Framework Ver 2.0			Cyber/Physical Security Framework Ver 1.1	
Function	Subcategory-ID	Subcategory	Measure Requirement ID	Measure Requirement
Detect (DE)	DE.CM-01	Networks and network services are monitored to find potentially adverse events	CPS.DE.CM-01	The organization monitors networks and network services to properly detect security events.
	DE.CM-02	The physical environment is monitored to find potentially adverse events	CPS.DE.CM-05	The organization implements appropriate physical access settings, logging, and monitoring, commensurate with the criticality of IoT devices, servers, and related assets.
	DE.CM-03	Personnel activity and technology usage are monitored to find potentially adverse events	CPS.DE.CM-04	The organization monitors the activities of internal and external personnel, including their access to and operations on elements (components, systems, etc.), to properly detect security events.
	DE.CM-06	External service provider activities and services are monitored to find potentially adverse events	CPS.DE.CM-03	The organization monitors communications with external service providers to properly detect security events.
	DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	CPS.DE.CM-02	The organization monitors the operational status of hardware and software across IoT devices, servers, and related assets, as well as network connection status, to properly detect security events.
	DE.AE-02	Potentially adverse events are analyzed to better understand associated activities	CPS.DE.AE-01	The organization analyzes potential security events to understand their details.
	DE.AE-03	Information is correlated from multiple sources	CPS.DE.AE-02	The organization accurately identifies security incidents by implementing procedures to correlate security events and analyze them against external threat information.
	DE.AE-04	The estimated impact and scope of adverse events are understood	CPS.DE.AE-03	The organization identifies the impact of security events, including the adverse effects on relevant external organizations.
	DE.AE-06	Information on adverse events is provided to authorized staff and tools	CPS.GV.RR-03	The organization appoints a security manager, establishes a security response organization (SOC/CSIRT), and maintains a structure to detect, analyze, and respond to security incidents within the organization.
	DE.AE-07	Cyber threat intelligence and other contextual information are integrated into the analysis	CPS.DE.AE-02	The organization accurately identifies security incidents by implementing procedures to correlate security events and analyze them against external threat information.
	DE.AE-08	Incidents are declared when adverse events meet the defined incident criteria	CPS.DE.AE-04	The organization establishes criteria for determining whether a security event constitutes an incident, and declares an incident when the criteria are met.
Respond (RS)	RS.MA-01	The incident response plan is executed in coordination with relevant third parties once an incident is declared	CPS.RS.MA-04	Once a security incident is declared, the organization executes incident response in accordance with predefined procedures, coordinating with other relevant organizations such as business partners.
	RS.MA-02	Incident reports are triaged and validated	CPS.RS.MA-02	The organization verifies that events reported as security incidents are not false positives or duplicate reports, and validates their legitimacy as incidents.
	RS.MA-03	Incidents are categorized and prioritized	CPS.RS.MA-03	The organization classifies and prioritizes detected security incidents based on the severity of impact, entry route, and other factors.
	RS.MA-04	Incidents are escalated or elevated as needed	CPS.RS.CO-02	Based on established rules, the organization escalates incidents to executive decision-makers within the organization and relevant external entities as necessary.
	RS.MA-05	The criteria for initiating incident recovery are applied	CPS.RS.MA-06	The organization determines the initiation of recovery based on predetermined criteria, taking into account the characteristics of the security incident and the impact of recovery activities on business operations.
	RS.AN-03	Analysis is performed to establish what has taken place during an incident and the root cause of the incident	CPS.RS.AN-02	After a security incident occurs, the organization conducts digital forensics to identify the root cause. In doing so, it preserves records of the investigation process in a tamper-resistant manner.
	RS.AN-06	Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved	CPS.RS.AN-02	After a security incident occurs, the organization conducts digital forensics to identify the root cause. In doing so, it preserves records of the investigation process in a tamper-resistant manner.
	RS.AN-07	Incident data and metadata are collected, and their integrity and provenance are preserved	CPS.RS.AN-01	The organization collects data and metadata related to security incidents (including the history of actions taken during incident response), preserves their integrity, and retains them in a state where acquisition sources, timestamps, and related provenance can be referenced.
	RS.AN-08	An incident's magnitude is estimated and validated	CPS.RS.AN-03	Based on the full scope of the security incident and the inferred intent of the threat actor, the organization assesses the impact on society as a whole, including the organization itself and relevant external organizations.
	RS.CO-02	Internal and external stakeholders are notified of incidents	CPS.RS.CO-01	The organization develops and implements rules governing internal communication and external disclosure after the occurrence of a security incident.
	RS.CO-03	Information is shared with designated internal and external stakeholders	CPS.RS.CO-01	The organization develops and implements rules governing internal communication and external disclosure after the occurrence of a security incident.
	RS.MI-01	Incidents are contained	CPS.RS.MI-01	The organization minimizes the spread of damage from security incidents, eradicating causes or mitigating adverse impacts.
	RS.MI-02	Incidents are eradicated	CPS.RS.MI-01	The organization minimizes the spread of damage from security incidents, eradicating causes or mitigating adverse impacts.
Recover (RC)	RC.RP-01	The recovery portion of the incident response plan is executed once initiated from the incident response process	CPS.RC.RP-03	Upon deciding to initiate the recovery phase, the organization executes recovery based on predetermined recovery plans.
	RC.RP-02	Recovery actions are selected, scoped, prioritized, and performed	CPS.RC.RP-03	Upon deciding to initiate the recovery phase, the organization executes recovery based on predetermined recovery plans.
	RC.RP-03	The integrity of backups and other restoration assets is verified before using them for restoration	CPS.RC.RP-04	The organization verifies the integrity of backups and other recovery assets prior to use.
	RC.RP-04	Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms	CPS.RC.RP-02	The organization takes into account critical business functions and the results of cybersecurity risk management when establishing post-incident operational policies.
	RC.RP-05	The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed	CPS.RC.RP-05	The organization verifies the integrity of restored assets, recovers systems and services, and confirms that they are in a normal operational state.
	RC.RP-06	The end of incident recovery is declared based on criteria, and incident-related documentation is completed	CPS.RC.RP-06	The organization declares the completion of incident recovery based on predetermined criteria and completes the documentation related to the incident.
	RC.CO-03	Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders	CPS.RC.CO-03	The organization specifies within its business continuity or emergency response plans that recovery activities must be communicated to internal and external stakeholders, officers, and management.
	RC.CO-04	Public updates on incident recovery are shared using approved methods and messaging	CPS.RC.CO-01	The organization establishes and maintains rules regarding information exchange aimed at recovery after the occurrence of a security incident.

D.2 Mapping NIST SP 800-171 (Rev.3) controls to Cyber/Physical Security Framework v1.1

NIST SP 800-171 (Rev.3)				NIST SP 800-53 (Rev.5 Release 5.1.1) Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework Ver 1.1	
FAMILY	ID	Category	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement
Access Control	03.01.01	Account Management	a. Define the types of system accounts allowed and prohibited.	- AC-02 Account Management - AC-02(03) Account Management Disable Accounts - AC-02(05) Account Management Inactivity Logout - AC-02(13) Account Management Disable Accounts for High-Risk Individuals	CPS.PR.AA-01	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.
			b. Create, enable, modify, disable, and remove system accounts in accordance with policy, procedures, prerequisites, and criteria.		CPS.PR.AA-05	The organization defines rules regarding the granting of access privileges in its security policies and incorporates the principles of least privilege and separation of duties.
			c. Specify: 1. Authorized users of the system, 2. Group and role membership, and 3. Access authorizations (i.e., privileges) for each account.		CPS.PR.AA-01	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.
			d. Authorize access to the system based on: 1. A valid access authorization and 2. Intended system usage.		CPS.PR.AA-01	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.
			e. Monitor the use of system accounts.		CPS.PR.AA-05	The organization defines rules regarding the granting of access privileges in its security policies and incorporates the principles of least privilege and separation of duties.
			f. Disable system accounts when: 1. The accounts have expired, 2. The accounts have been inactive for [Assignment: organization-defined time period], 3. The accounts are no longer associated with a user or individual, 4. The accounts are in violation of organizational policy, or 5. Significant risks associated with individuals are discovered.		CPS.PR.AA-02	The organization authenticates and authorizes logical access to components (physical items, systems, etc.) by IoT devices and users using highly reliable methods (e.g., multi-factor authentication) commensurate with transaction risks (personal security, privacy risks, and other organizational risks).
			g. Notify account managers and designated personnel or roles within: 1. [Assignment: organization-defined time period] when accounts are no longer required. 2. [Assignment: organization-defined time period] when users are terminated or transferred. 3. [Assignment: organization-defined time period] when system usage or the need-to-know changes for an individual.		CPS.PR.PS-11	To appropriately detect security incidents, the organization determines and documents the scope and types of events for audit logging, and continuously records and reviews logs.
			h. Require that users log out of the system after [Assignment: organization-defined time period] of expected inactivity or when [Assignment: organization-defined circumstances].		CPS.DE.CM-04	The organization monitors the activities of internal and external personnel, including their access to and operations on elements (components, systems, etc.), to properly detect security events.
					CPS.GV.RR-05	The organization incorporates security-related matters (e.g., revoking access privileges and screening employees) into measures that address role changes resulting from personnel transfers.
					CPS.PR.AA-01	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.
					CPS.PR.AA-06	The organization periodically reviews granted access privileges and remediates unnecessary or excessive permissions.
					CPS.GV.RR-05	The organization incorporates security-related matters (e.g., revoking access privileges and screening employees) into measures that address role changes resulting from personnel transfers.
					—	—
	03.01.02	Access Enforcement	Enforce approved authorizations for logical access to CUI and system resources in accordance with applicable access control policies.	- AC-03 Access Enforcement - AC-17 Remote Access	CPS.PR.AA-02	The organization authenticates and authorizes logical access to components (physical items, systems, etc.) by IoT devices and users using highly reliable methods (e.g., multi-factor authentication) commensurate with transaction risks (personal security, privacy risks, and other organizational risks).
					CPS.PR.AA-05	The organization defines rules regarding the granting of access privileges in its security policies and incorporates the principles of least privilege and separation of duties.
	03.01.03	Information Flow Enforcement	Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems.	AC-04 Information Flow Enforcement	CPS.PR.IR-01	The organization protects networks and environments from unauthorized access and use by implementing network segmentation (e.g., separating development/test environments from production environments, and isolating IoT device environments from other networks within the organization).
	03.01.04	Separation of Duties	a. Identify the duties of individuals requiring separation.	AC-05 Separation of Duties	CPS.PR.AA-05	The organization defines rules regarding the granting of access privileges in its security policies and incorporates the principles of least privilege and separation of duties.
			b. Define system access authorizations to support separation of duties.		—	—

NIST SP 800-171 (Rev.3)				NIST SP 800-53 (Rev.5 Release 5.1.1) Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework Ver 1.1	
FAMILY	ID	Category	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement
	03.01.05	Least Privilege	a. Allow only authorized system access for users (or processes acting on behalf of users) that is necessary to accomplish assigned organizational tasks.	- AC-06 Least Privilege - AC-06(01) Least Privilege Authorize Access to Security Functions - AC-06(07) Least Privilege Review of User Privileges	CPS.PR.AA-05	The organization defines rules regarding the granting of access privileges in its security policies and incorporates the principles of least privilege and separation of duties.
			b. Authorize access to [Assignment: organization-defined security functions] and [Assignment: organization-defined security-relevant information].		CPS.PR.AA-05	The organization defines rules regarding the granting of access privileges in its security policies and incorporates the principles of least privilege and separation of duties.
			c. Review the privileges assigned to roles or classes of users [Assignment: organization-defined frequency] to validate the need for such privileges.		CPS.PR.AA-06	The organization periodically reviews granted access privileges and remediates unnecessary or excessive permissions.
			d. Reassign or remove privileges, as necessary.		CPS.PR.AA-06	The organization periodically reviews granted access privileges and remediates unnecessary or excessive permissions.
	03.01.06	Least Privilege – Privileged Accounts	a. Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].	- AC-06(02) Least Privilege Non-Privileged Access for Non-Security Functions - AC-06(05) Least Privilege Privileged Accounts	CPS.PR.AA-05	The organization defines rules regarding the granting of access privileges in its security policies and incorporates the principles of least privilege and separation of duties.
			b. Require that users (or roles) with privileged accounts use non-privileged accounts when accessing non-security functions or non-security information.		—	—
	03.01.07	Least Privilege – Privileged Functions	a. Prevent non-privileged users from executing privileged functions.	- AC-06(09) Least Privilege Log Use of Privileged Functions - AC-06(10) Least Privilege Prohibit Non-Privileged Users From Executing Privileged Functions	CPS.PR.AA-05	The organization defines rules regarding the granting of access privileges in its security policies and incorporates the principles of least privilege and separation of duties.
			b. Log the execution of privileged functions.		CPS.PR.PS-11	To appropriately detect security incidents, the organization determines and documents the scope and types of events for audit logging, and continuously records and reviews logs.
	03.01.08	Unsuccessful Logon Attempts	a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period].	AC-07 Unsuccessful Logon Attempts	CPS.PR.AA-03	The organization prevents unauthorized logins to IoT devices, servers, and related assets by implementing mechanisms such as account lockout after a specified number of failed authentication attempts and enforcing delays on subsequent login attempts until security conditions are verified.
			b. Automatically [Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt; notify system administrator; take other action] when the maximum number of unsuccessful attempts is exceeded.		CPS.PR.AA-03	The organization prevents unauthorized logins to IoT devices, servers, and related assets by implementing mechanisms such as account lockout after a specified number of failed authentication attempts and enforcing delays on subsequent login attempts until security conditions are verified.
	03.01.09	System Use Notification	Display a system use notification message with privacy and security notices consistent with applicable CUI rules before granting access to the system.	AC-08 System Use Notification	—	—
	03.01.10	Device Lock	a. Prevent access to the system by [Selection (one or more): initiating a device lock after [Assignment: organization-defined time period] of inactivity; requiring the user to initiate a device lock before leaving the system unattended].	- AC-11 Device Lock - AC-11(01) Device Lock Pattern-Hiding Displays	—	—
			b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.		—	—
			c. Conceal, via the device lock, information previously visible on the display with a publicly viewable image.		—	—
	03.01.11	Session Termination	Terminate a user session automatically after [Assignment: organization-defined conditions or trigger events requiring session disconnect].	AC-12 Session Termination	—	—
	03.01.12	Remote Access	a. Establish usage restrictions, configuration requirements, and connection requirements for each type of allowable remote system access.	- AC-17(03) Remote Access Managed Access Control Points - AC-17(04) Remote Access Privileged Commands and Access	—	—
			b. Authorize each type of remote system access prior to establishing such connections.		CPS.PR.AA-02	The organization authenticates and authorizes logical access to components (physical items, systems, etc.) by IoT devices and users using highly reliable methods (e.g., multi-factor authentication) commensurate with transaction risks (personal security, privacy risks, and other organizational risks).
			c. Route remote access to the system through authorized and managed access control points.		CPS.PR.IR-01	The organization protects networks and environments from unauthorized access and use by implementing network segmentation (e.g., separating development/test environments from production environments, and isolating IoT device environments from other networks within the organization).
			d. Authorize the remote execution of privileged commands and remote access to security-relevant information.		CPS.PR.AA-02	The organization authenticates and authorizes logical access to components (physical items, systems, etc.) by IoT devices and users using highly reliable methods (e.g., multi-factor authentication) commensurate with transaction risks (personal security, privacy risks, and other organizational risks).

NIST SP 800-171 (Rev.3)				NIST SP 800-53 (Rev.5 Release 5.1.1) Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework Ver 1.1	
FAMILY	ID	Category	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement
	03.01.13	Withdrawn	Addressed by 03.13.08.			
	03.01.14	Withdrawn	Incorporated into 03.01.12.			
	03.01.15	Withdrawn	Incorporated into 03.01.12.			
	03.01.16	Wireless Access	a. Establish usage restrictions, configuration requirements, and connection requirements for each type of wireless access to the system.	- AC-18 Wireless Access - AC-18(01) Wireless Access Authentication and Encryption - AC-18(03) Wireless Access Disable Wireless Networking	—	—
			b. Authorize each type of wireless access to the system prior to establishing such connections.		CPS.PR.AA-02	The organization authenticates and authorizes logical access to components (physical items, systems, etc.) by IoT devices and users using highly reliable methods (e.g., multi-factor authentication) commensurate with transaction risks (personal security, privacy risks, and other organizational risks).
			c. Disable, when not intended for use, wireless networking capabilities prior to issuance and deployment.		CPS.PR.PS-06	The organization establishes and applies configuration management practices for hardware and software of IoT devices, servers, and related assets (including minimizing functionality by physically or logically disabling unnecessary network, USB, and serial ports).
			d. Protect wireless access to the system using authentication and encryption.		CPS.PR.AA-02	The organization authenticates and authorizes logical access to components (physical items, systems, etc.) by IoT devices and users using highly reliable methods (e.g., multi-factor authentication) commensurate with transaction risks (personal security, privacy risks, and other organizational risks).
					CPS.PR.DS-03	The organization protects the confidentiality, integrity, and availability of data-in-transit.
	03.01.17	Withdrawn	Incorporated into 03.01.16.			
	03.01.18	Access Control for Mobile Devices	a. Establish usage restrictions, configuration requirements, and connection requirements for mobile devices.	- AC-19 Access Control for Mobile Devices - AC-19(05) Access Control for Mobile Devices Full Device or Container Based Encryption	—	—
			b. Authorize the connection of mobile devices to the system.		CPS.PR.AA-02	The organization authenticates and authorizes logical access to components (physical items, systems, etc.) by IoT devices and users using highly reliable methods (e.g., multi-factor authentication) commensurate with transaction risks (personal security, privacy risks, and other organizational risks).
			c. Implement full-device or container-based encryption to protect the confidentiality of CUI on mobile devices.		CPS.PR.DS-02	The organization protects the confidentiality, integrity, and availability of data-at-rest.
	03.01.19	Withdrawn	Incorporated into 03.01.18.			
	03.01.20	Use of External Systems	a. Prohibit the use of external systems unless the systems are specifically authorized.	- AC-20 Use of External Systems - AC-20(01) Use of External Systems Limits on Authorized Use - AC-20(02) Use of External Systems Portable Storage Devices – Restricted Use	—	—
			b. Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assignment: organization-defined security requirements].		CPS.GV.SC-05	The organization establishes supply chain cybersecurity standards considering the lifecycle of business relationships, clearly defines the scope of responsibilities, and agrees on them with partners through contracts or other means.
			c. Permit authorized individuals to use external systems to access the organizational system or to process, store, or transmit CUI only after: - Verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied and - Retaining approved system connection or processing agreements with the organizational entities hosting the external systems.		CPS.GV.SC-05	The organization establishes supply chain cybersecurity standards considering the lifecycle of business relationships, clearly defines the scope of responsibilities, and agrees on them with partners through contracts or other means.
			d. Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.		CPS.GV.SC-07	When entering into contracts with other relevant organizations such as business partners, the organization considers its objectives and risk management outcomes, verifying that products and services provided by them conform to the organization's security requirements.
					—	—
	03.01.21	Withdrawn	Incorporated into 03.01.20.			
	03.01.22	Publicly Accessible Content	a. Train authorized individuals to ensure that publicly accessible information does not contain CUI.	AC-22 Publicly Accessible Content	CPS.PR.AT-01	The organization conducts appropriate training and education for all personnel to carry out their assigned roles and responsibilities to minimize the occurrence and impact of security incidents, and maintains records of such activities.
			b. Review the content on publicly accessible systems for CUI and remove such information, if discovered.		—	—

NIST SP 800-171 (Rev.3)				NIST SP 800-53 (Rev.5 Release 5.1.1) Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework Ver 1.1	
FAMILY	ID	Category	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement
Awareness and Training	03.02.01	Literacy Training and Awareness	a. Provide security literacy training to system users: 1. As part of initial training for new users and [Assignment: organization defined frequency] thereafter, 2. When required by system changes or following [Assignment: organization defined events], and 3. On recognizing and reporting indicators of insider threat, social engineering, and social mining.	· AT-02 Literacy Training and Awareness · AT-02(02) Literacy Training and Awareness Insider Threat · AT-02(03) Literacy Training and Awareness Social Engineering and Mining	CPS.PR.AT-01	The organization conducts appropriate training and education for all personnel to carry out their assigned roles and responsibilities to minimize the occurrence and impact of security incidents, and maintains records of such activities.
			b. Update security literacy training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].		CPS.ID.IM-03	The organization continuously improves security training and education programs for its personnel and designated contacts at critical partner organizations.
	03.02.02	Role-Based Training	a. Provide role-based security training to organizational personnel: 1. Before authorizing access to the system or CUI, before performing assigned duties, and [Assignment: organization-defined frequency] thereafter 2. When required by system changes or following [Assignment: organization defined events].	· AT-03 Role-Based Training	CPS.PR.AT-01	The organization conducts appropriate training and education for all personnel to carry out their assigned roles and responsibilities to minimize the occurrence and impact of security incidents, and maintains records of such activities.
			b. Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].		CPS.ID.IM-03	The organization continuously improves security training and education programs for its personnel and designated contacts at critical partner organizations.
	03.02.03	Withdrawn	Incorporated into 03.02.01.			
Audit and Accountability	03.03.01	Event Logging	a. Specify the following event types selected for logging within the system: [Assignment: organization-defined event types].	· AU-02 Event Logging	CPS.PR.PS-11	To appropriately detect security incidents, the organization determines and documents the scope and types of events for audit logging, and continuously records and reviews logs.
			b. Review and update the event types selected for logging [Assignment: organization-defined frequency].		CPS.PR.PS-11	To appropriately detect security incidents, the organization determines and documents the scope and types of events for audit logging, and continuously records and reviews logs.
	03.03.02	Audit Record Content	a. Include the following content in audit records: 1. What type of event occurred 2. When the event occurred 3. Where the event occurred 4. Source of the event 5. Outcome of the event 6. Identity of the individuals, subjects, objects, or entities associated with the event	· AU-03 Content of Audit Records · AU-03(01) Additional Audit Information	CPS.PR.PS-11	To appropriately detect security incidents, the organization determines and documents the scope and types of events for audit logging, and continuously records and reviews logs.
			b. Provide additional information for audit records as needed.		CPS.PR.PS-11	To appropriately detect security incidents, the organization determines and documents the scope and types of events for audit logging, and continuously records and reviews logs.
	03.03.03	Audit Record Generation	a. Generate audit records for the selected event types and audit record content specified in 03.03.01 and 03.03.02.	· AU-11 Audit Record Retention · AU-12 Audit Record Generation	CPS.PR.PS-11	To appropriately detect security incidents, the organization determines and documents the scope and types of events for audit logging, and continuously records and reviews logs.
			b. Retain audit records for a time period consistent with the records retention policy.		CPS.PR.PS-11	To appropriately detect security incidents, the organization determines and documents the scope and types of events for audit logging, and continuously records and reviews logs.
	03.03.04	Response to Audit Logging Process Failures	a. Alert organizational personnel or roles within [Assignment: organization-defined time period] in the event of an audit logging process failure.	· AU-05 Response to Audit Logging Process Failures	—	—
			b. Take the following additional actions: [Assignment: organization-defined additional actions].		—	—
	03.03.05	Audit Record Review, Analysis, and Reporting	a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications and the potential impact of inappropriate or unusual activity.	· AU-06 Audit Record Review, Analysis, and Reporting · AU-06(03) Audit Record Review, Analysis, and Reporting Correlate Audit Record Repositories	CPS.PR.PS-11	To appropriately detect security incidents, the organization determines and documents the scope and types of events for audit logging, and continuously records and reviews logs.
			b. Report findings to organizational personnel or roles.		CPS.DE.AE-01	The organization analyzes potential security events to understand their details.
			c. Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.		CPS.PR.PS-11	To appropriately detect security incidents, the organization determines and documents the scope and types of events for audit logging, and continuously records and reviews logs.
					CPS.DE.AE-02	The organization accurately identifies security incidents by implementing procedures to correlate security events and analyze them against external threat information.
	03.03.06	Audit Record Reduction and Report Generation	a. Implement an audit record reduction and report generation capability that supports audit record review, analysis, reporting requirements, and after-the-fact investigations of incidents.	· AU-07 Audit Record Reduction and Report Generation	—	—
					—	—
			b. Preserve the original content and time ordering of audit records.		—	—

NIST SP 800-171 (Rev.3)				NIST SP 800-53 (Rev.5 Release 5.1.1) Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework Ver 1.1	
FAMILY	ID	Category	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement
	03.03.07	Time Stamps	a. Use internal system clocks to generate time stamps for audit records.	· AU-08 Time Stamps	—	—
			b. Record time stamps for audit records that meet [Assignment: organization defined granularity of time measurement] and that use Coordinated Universal Time (UTC), have a fixed local time offset from UTC, or include the local time offset as part of the time stamp.		—	—
	03.03.08	Protection of Audit Information	a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	· AU-09 Protection of Audit Information · AU-09(04) Protection of Audit Information Access by Subset of Privileged Users	CPS.PR.DS-02	The organization protects the confidentiality, integrity, and availability of data-at-rest.
			b. Authorize access to management of audit logging functionality to only a subset of privileged users or roles.		CPS.PR.AA-05	The organization defines rules regarding the granting of access privileges in its security policies and incorporates the principles of least privilege and separation of duties.
	03.03.09	Withdrawn	Incorporated into 03.03.08.			
Configuration Management	03.04.01	Baseline Configuration	a. Develop and maintain under configuration control, a current baseline configuration of the system.	· CM-02 Baseline Configuration	CPS.PR.PS-06	The organization establishes and applies configuration management practices for hardware and software of IoT devices, servers, and related assets (including minimizing functionality by physically or logically disabling unnecessary network, USB, and serial ports).
			b. Review and update the baseline configuration of the system [Assignment: organization-defined frequency] and when system components are installed or modified.		—	—
	03.04.02	Configuration Settings	a. Establish, document, and implement the following configuration settings for the system that reflect the most restrictive mode consistent with operational requirements: [Assignment: organization-defined configuration settings].	· CM-06 Configuration Settings	CPS.PR.PS-06	The organization establishes and applies configuration management practices for hardware and software of IoT devices, servers, and related assets (including minimizing functionality by physically or logically disabling unnecessary network, USB, and serial ports).
			b. Identify, document, and approve any deviations from established configuration settings.		CPS.ID.RA-07	The organization assesses the risk impact posed by significant organizational changes and security requirement exceptions, and records and manages the results.
	03.04.03	Configuration Change Control	a. Define the types of changes to the system that are configuration-controlled.	· CM-03 Configuration Change Control	CPS.PR.PS-06	The organization establishes and applies configuration management practices for hardware and software of IoT devices, servers, and related assets (including minimizing functionality by physically or logically disabling unnecessary network, USB, and serial ports).
			b. Review proposed configuration-controlled changes to the system, and approve or disapprove such changes with explicit consideration for security impacts.		CPS.ID.RA-07	The organization assesses the risk impact posed by significant organizational changes and security requirement exceptions, and records and manages the results.
			c. Implement and document approved configuration-controlled changes to the system.		CPS.PR.PS-06	The organization establishes and applies configuration management practices for hardware and software of IoT devices, servers, and related assets (including minimizing functionality by physically or logically disabling unnecessary network, USB, and serial ports).
			d. Monitor and review activities associated with configuration-controlled changes to the system.		—	—
	03.04.04	Impact Analyses	a. Analyze changes to the system to determine potential security impacts prior to change implementation.	· CM-04 Impact Analyses · CM-04(02) Impact Analyses Verification of Controls	CPS.ID.RA-07	The organization assesses the risk impact posed by significant organizational changes and security requirement exceptions, and records and manages the results.
			b. Verify that the security requirements for the system continue to be satisfied after the system changes have been implemented.		—	—
	03.04.05	Access Restrictions for Change	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.	· CM-05 Access Restrictions for Change	CPS.PR.AA-05	The organization defines rules regarding the granting of access privileges in its security policies and incorporates the principles of least privilege and separation of duties.
					CPS.PR.AA-07	The organization implements physical safeguards, such as locking installation areas for IoT devices, servers, and related assets, controlling entry and exit, deploying biometric authentication, installing surveillance cameras, and conducting baggage and weight inspections.

NIST SP 800-171 (Rev.3)				NIST SP 800-53 (Rev.5 Release 5.1.1) Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework Ver 1.1	
FAMILY	ID	Category	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement
	03.04.06	Least Functionality	a. Configure the system to provide only mission-essential capabilities.	- CM-07 Least Functionality - CM-07(01) Least Functionality Periodic Review	CPS.PR.PS-06	The organization establishes and applies configuration management practices for hardware and software of IoT devices, servers, and related assets (including minimizing functionality by physically or logically disabling unnecessary network, USB, and serial ports).
			b. Prohibit or restrict use of the following functions, ports, protocols, connections, and services: [Assignment: organization-defined functions, ports, protocols, connections, and services].		CPS.PR.PS-06	The organization establishes and applies configuration management practices for hardware and software of IoT devices, servers, and related assets (including minimizing functionality by physically or logically disabling unnecessary network, USB, and serial ports).
			c. Review the system [Assignment: organization-defined frequency] to identify unnecessary or nonsecure functions, ports, protocols, connections, and services.		—	—
			d. Disable or remove functions, ports, protocols, connections, and services that are unnecessary or nonsecure.		CPS.PR.PS-06	The organization establishes and applies configuration management practices for hardware and software of IoT devices, servers, and related assets (including minimizing functionality by physically or logically disabling unnecessary network, USB, and serial ports).
	03.04.07	Withdrawn	Incorporated into 03.04.06 and 03.04.08.			
	03.04.08	Authorized Software – Allow by Exception	a. Identify software programs authorized to execute on the system.	CM-07(05) Least Functionality Authorized Software – Allow by Exception	CPS.ID.AM-06	The organization manages systems, hardware, software, services, and data throughout their entire lifecycle, from acquisition to disposal.
			b. Implement a deny-all, allow-by-exception policy for the execution of authorized software programs on the system.		CPS.PR.PS-07	The organization prevents the installation and execution of unauthorized software.
			c. Review and update the list of authorized software programs [Assignment: organization-defined frequency].		—	—
	03.04.09	Withdrawn	Addressed by 03.01.05, 03.01.06, 03.01.07, 03.04.08, and 03.12.03.			
	03.04.10	System Component Inventory	a. Develop and document an inventory of system components.	- CM-08 System Component Inventory - CM-08(01) System Component Inventory Updates During Installation and Removal	CPS.ID.AM-01	The organization develops and appropriately manages inventories of hardware, software, and their management information (e.g., name, version, network address, designated manager, and license information) that comprise its system.
			b. Review and update the system component inventory [Assignment: organization defined frequency].		CPS.ID.AM-01	The organization develops and appropriately manages inventories of hardware, software, and their management information (e.g., name, version, network address, designated manager, and license information) that comprise its system.
			c. Update the system component inventory as part of installations, removals, and system updates.		CPS.ID.AM-06	The organization manages systems, hardware, software, services, and data throughout their entire lifecycle, from acquisition to disposal.
	03.04.11	Information Location	a. Identify and document the location of CUI and the system components on which the information is processed and stored.	CM-12 Information Location	CPS.ID.AM-05	The organization develops and appropriately manages inventories of data and metadata in its possession.
			b. Document changes to the system or system component location where CUI is processed and stored.		—	—
	03.04.12	System and Component Configuration for High-Risk Areas	a. Issue systems or system components with the following configurations to individuals traveling to high-risk locations: [Assignment: organization-defined system configurations].	CM-02(07) Baseline Configuration Configure Systems and Components for High-Risk Areas	—	—
			b. Apply the following security requirements to the systems or components when the individuals return from travel: [Assignment: organization-defined security requirements].		—	—
Identification and Authentication	03.05.01	User Identification and Authentication	a. Uniquely identify and authenticate system users, and associate that unique identification with processes acting on behalf of those users.	- IA-02 Identification and Authentication (Organizational Users) - IA-11 Re-Authentication	CPS.PR.AA-02	The organization authenticates and authorizes logical access to components (physical items, systems, etc.) by IoT devices and users using highly reliable methods (e.g., multi-factor authentication) commensurate with transaction risks (personal security, privacy risks, and other organizational risks).
			b. Re-authenticate users when [Assignment: organization-defined circumstances or situations requiring re-authentication].		—	—
	03.05.02	Device Identification and Authentication	Uniquely identify and authenticate [Assignment: organization-defined devices or types of devices] before establishing a system connection.	IA-03 Device Identification and Authentication	CPS.PR.AA-02	The organization authenticates and authorizes logical access to components (physical items, systems, etc.) by IoT devices and users using highly reliable methods (e.g., multi-factor authentication) commensurate with transaction risks (personal security, privacy risks, and other organizational risks).
	03.05.03	Multi-Factor Authentication	Implement multi-factor authentication for access to privileged and non-privileged accounts.	- IA-02(01) Identification and Authentication (Organizational Users) Multi-Factor Authentication to Privileged Accounts - IA-02(02) Identification and Authentication (Organizational Users) Multi-Factor Authentication to Non-Privileged Accounts	CPS.PR.AA-02	The organization authenticates and authorizes logical access to components (physical items, systems, etc.) by IoT devices and users using highly reliable methods (e.g., multi-factor authentication) commensurate with transaction risks (personal security, privacy risks, and other organizational risks).
	03.05.04	Replay-Resistant Authentication	Implement replay-resistant authentication mechanisms for access to privileged and non-privileged accounts.	IA-02(08) Identification and Authentication (Organizational Users) Access to Accounts – Replay Resistant	CPS.PR.AA-02	The organization authenticates and authorizes logical access to components (physical items, systems, etc.) by IoT devices and users using highly reliable methods (e.g., multi-factor authentication) commensurate with transaction risks (personal security, privacy risks, and other organizational risks).

NIST SP 800-171 (Rev.3)				NIST SP 800-53 (Rev.5 Release 5.1.1) Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework Ver 1.1	
FAMILY	ID	Category	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement
	03.05.05	Identifier Management	a. Receive authorization from organizational personnel or roles to assign an individual, group, role, service, or device identifier.	- IA-04 Identifier Management - IA-04(04) Identifier Management Identify User Status	—	—
			b. Select and assign an identifier that identifies an individual, group, role, service, or device.		CPS.PR.AA-01	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.
			c. Prevent the reuse of identifiers for [Assignment: organization-defined time period].		CPS.PR.AA-01	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.
			d. Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].		CPS.PR.AA-01	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.
	03.05.06	Withdrawn	Consistency with SP 800-53 [8].			
	03.05.07	Password Management	a. Maintain a list of commonly-used, expected, or compromised passwords, and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised.	IA-05(01) Authenticator Management Password-Based Authentication	—	—
			b. Verify that passwords are not found on the list of commonly used, expected, or compromised passwords when users create or update passwords.		—	—
			c. Transmit passwords only over cryptographically protected channels.		CPS.PR.DS-03	The organization protects the confidentiality, integrity, and availability of data-in-transit.
			d. Store passwords in a cryptographically protected form.		CPS.PR.DS-02	The organization protects the confidentiality, integrity, and availability of data-at-rest.
			e. Select a new password upon first use after account recovery.		—	—
			f. Enforce the following composition and complexity rules for passwords: [Assignment: organization-defined composition and complexity rules].		—	—
	03.05.08	Withdrawn	Consistency with SP 800-53 [8].			
	03.05.09	Withdrawn	Consistency with SP 800-53 [8].			
	03.05.10	Withdrawn	Incorporated into 03.05.07.			
	03.05.11	Authentication Feedback	Obscure feedback of authentication information during the authentication process.	IA-06 Authentication Feedback	—	—
	03.05.12	Authenticator Management	a. Verify the identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution.	IA-05 Authenticator Management	CPS.PR.AA-01	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.
			b. Establish initial authenticator content for any authenticators issued by the organization.		CPS.PR.AA-01	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.
			c. Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.		CPS.PR.AA-01	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.
			d. Change default authenticators at first use.		CPS.PR.AA-01	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.
			e. Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events].		CPS.PR.AA-01	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.
			f. Protect authenticator content from unauthorized disclosure and modification.		CPS.PR.DS-02	The organization protects the confidentiality, integrity, and availability of data-at-rest.
Incident Response	03.06.01	Incident Handling	Implement an incident-handling capability that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.	IR-04 Incident Handling	CPS.GV.RR-03	The organization appoints a security manager, establishes a security response organization (SOC/CSIRT), and maintains a structure to detect, analyze, and respond to security incidents within the organization.
					CPS.RS.MA-01	To clarify response actions, priorities, and remediation scope following the occurrence of a security incident, the organization predefines and implements response procedures (security operation processes) for the organization, people, components, and systems after detecting an incident.

NIST SP 800-171 (Rev.3)				NIST SP 800-53 (Rev.5 Release 5.1.1) Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework Ver 1.1	
FAMILY	ID	Category	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement
	03.06.02	Incident Monitoring, Reporting, and Response Assistance	a. Track and document system security incidents.	• IR-05 Incident Monitoring • IR-06 Incident Reporting • IR-07 Incident Response Assistance	CPS.RS.AN-01	The organization collects data and metadata related to security incidents (including the history of actions taken during incident response), preserves their integrity, and retains them in a state where acquisition sources, timestamps, and related provenance can be referenced.
			b. Report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period].		CPS.RS.MA-02	The organization verifies that events reported as security incidents are not false positives or duplicate reports, and validates their legitimacy as incidents.
			c. Report incident information to [Assignment: organization-defined authorities].		CPS.RS.CO-02	Based on established rules, the organization escalates incidents to executive decision-makers within the organization and relevant external entities as necessary.
			d. Provide an incident response support resource that offers advice and assistance to system users on handling and reporting incidents.		CPS.GV.RR-03	The organization appoints a security manager, establishes a security response organization (SOC/CSIRT), and maintains a structure to detect, analyze, and respond to security incidents within the organization.
	03.06.03	Incident Response Testing	Test the effectiveness of the incident response capability [Assignment: organization defined frequency].	• IR-03 Incident Response Testing	CPS.PR.AT-01	The organization conducts appropriate training and education for all personnel to carry out their assigned roles and responsibilities to minimize the occurrence and impact of security incidents, and maintains records of such activities.
					CPS.PR.AT-02	The organization provides appropriate training and security education to designated personnel of external partners critical to security management, who may be involved in security incident response for the organization, enabling them to fulfill their assigned roles, and maintains records of such activities.
	03.06.04	Incident Response Training	a. Provide incident response training to system users consistent with assigned roles and responsibilities: 1. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility or acquiring system access, 2. When required by system changes, and 3. [Assignment: organization-defined frequency] thereafter.	• IR-02 Incident Response Training	CPS.PR.AT-01	The organization conducts appropriate training and education for all personnel to carry out their assigned roles and responsibilities to minimize the occurrence and impact of security incidents, and maintains records of such activities.
			b. Review and update incident response training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].		CPS.ID.IM-03	The organization continuously improves security training and education programs for its personnel and designated contacts at critical partner organizations.
	03.06.05	Incident Response Plan	a. Develop an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability, 2. Describes the structure and organization of the incident response capability, 3. Provides a high-level approach for how the incident response capability fits into the overall organization, 4. Defines reportable incidents, 5. Addresses the sharing of incident information, and 6. Designates responsibilities to organizational entities, personnel, or roles.	• IR-08 Incident Response Plan	CPS.GV.RR-02	The organization establishes roles, responsibilities, and authorities related to its cybersecurity risk management and communicates them within the organization.
			b. Distribute copies of the incident response plan to designated incident response personnel (identified by name and/or by role) and organizational elements.		CPS.RS.MA-01	To clarify response actions, priorities, and remediation scope following the occurrence of a security incident, the organization predefines and implements response procedures (security operation processes) for the organization, people, components, and systems after detecting an incident.
					CPS.RS.CO-01	The organization develops and implements rules governing internal communication and external disclosure after the occurrence of a security incident.
					—	—
			c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing.		CPS.ID.IM-06	The organization incorporates lessons learned from responses to security incidents to continuously improve its incident response plan.
			d. Protect the incident response plan from unauthorized disclosure.		CPS.PR.DS-02	The organization protects the confidentiality, integrity, and availability of data-at-rest.
Maintenance	03.07.01	Withdrawn	Recategorized as NCO.			
	03.07.02	Withdrawn	Incorporated into 03.07.04 and 03.07.06.			
	03.07.03	Withdrawn	Incorporated into 03.08.03.			
	03.07.04	Maintenance Tools	a. Approve, control, and monitor the use of system maintenance tools.	• MA-03 Maintenance Tools • MA-03(01) Maintenance Tools Inspect Tools • MA-03(02) Maintenance Tools Inspect Media • MA-03(03) Maintenance Tools Prevent Unauthorized Removal	CPS.PR.PS-10	The organization performs maintenance on its own IoT devices, servers, and related assets with prior approval from the department that owns the target component or system, logging maintenance activities and preventing unauthorized access.
			b. Check media with diagnostic and test programs for malicious code before it is used in the system.		CPS.PR.PS-01	The organization evaluates the authenticity and integrity of hardware and software prior to acquisition and deployment, and verifies their integrity during operation.
			c. Prevent the removal of system maintenance equipment containing CUI by verifying that there is no CUI on the equipment, sanitizing or destroying the equipment, or retaining the equipment within the facility.		CPS.PR.DS-02	The organization protects the confidentiality, integrity, and availability of data-at-rest.

NIST SP 800-171 (Rev.3)				NIST SP 800-53 (Rev.5 Release 5.1.1) Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework Ver 1.1	
FAMILY	ID	Category	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement
	03.07.05	Nonlocal Maintenance	a. Approve and monitor nonlocal maintenance and diagnostic activities.	· MA-04 Nonlocal Maintenance	CPS.PR.PS-10	The organization performs maintenance on its own IoT devices, servers, and related assets with prior approval from the department that owns the target component or system, logging maintenance activities and preventing unauthorized access.
			b. Implement multi-factor authentication and replay resistance in the establishment of nonlocal maintenance and diagnostic sessions.		CPS.PR.AA-02	The organization authenticates and authorizes logical access to components (physical items, systems, etc.) by IoT devices and users using highly reliable methods (e.g., multi-factor authentication) commensurate with transaction risks (personal security, privacy risks, and other organizational risks).
			c. Terminate session and network connections when nonlocal maintenance is completed.		—	—
	03.07.06	Maintenance Personnel	a. Establish a process for maintenance personnel authorization.	· MA-05 Maintenance Personnel	—	—
			b. Maintain a list of authorized maintenance organizations or personnel.		CPS.PR.AA-01	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.
			c. Verify that non-escorted personnel who perform maintenance on the system possess the required access authorizations.		—	—
			d. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.		—	—
Media Protection	03.08.01	Media Storage	Physically control and securely store system media that contain CUI.	· MP-04 Media Storage	CPS.PR.DS-02	The organization protects the confidentiality, integrity, and availability of data-at-rest.
					CPS.PR.AA-07	The organization implements physical safeguards, such as locking installation areas for IoT devices, servers, and related assets, controlling entry and exit, deploying biometric authentication, installing surveillance cameras, and conducting baggage and weight inspections.
	03.08.02	Media Access	Restrict access to CUI on system media to authorized personnel or roles.	· MP-02 Media Access	CPS.PR.AA-05	The organization defines rules regarding the granting of access privileges in its security policies and incorporates the principles of least privilege and separation of duties.
					CPS.PR.AA-07	The organization implements physical safeguards, such as locking installation areas for IoT devices, servers, and related assets, controlling entry and exit, deploying biometric authentication, installing surveillance cameras, and conducting baggage and weight inspections.
	03.08.03	Media Sanitization	Sanitize system media that contain CUI prior to disposal, release out of organizational control, or release for reuse.	· MP-06 Media Sanitization	CPS.PR.PS-12	Upon the disposal of IoT devices, servers, and related assets, the organization deletes or renders unreadable all internally stored data, unique identifiers of legitimate devices and systems, and critical security information (e.g., private keys and digital certificates).
	03.08.04	Media Marking	Mark system media that contain CUI to indicate distribution limitations, handling caveats, and applicable CUI markings.	· MP-03 Media Marking	CPS.PR.DS-01	The organization accurately understands the required level of data protection mandated by various laws, regulations, and agreements regarding data shared exclusively among relevant organizations, establishes data classification methods based on respective requirements, and appropriately protects data commensurate with its classification throughout the entire lifecycle.
	03.08.05	Media Transport	a. Protect and control system media that contain CUI during transport outside of controlled areas.	· MP-05 Media Transport · SC-28 Protection of Information at Rest	—	—
			b. Maintain accountability of system media that contain CUI during transport outside of controlled areas.		—	—
			c. Document activities associated with the transport of system media that contain CUI.		—	—
	03.08.06	Withdrawn	Addressed by 03.13.08.			
	03.08.07	Media Use	a. Restrict or prohibit the use of [Assignment: organization-defined types of system media].	· MP-07 Media Use	CPS.ID.AM-06	The organization manages systems, hardware, software, services, and data throughout their entire lifecycle, from acquisition to disposal.
			b. Prohibit the use of removable system media without an identifiable owner.		—	—
	03.08.08	Withdrawn	Incorporated into 03.08.07.			

NIST SP 800-171 (Rev.3)				NIST SP 800-53 (Rev.5 Release 5.1.1) Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework Ver 1.1	
FAMILY	ID	Category	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement
	03.08.09	System Backup – Cryptographic Protection	a. Protect the confidentiality of backup information.	- CP-09 System Backup - CP-09(08) System Backup Cryptographic Protection	CPS.PR.DS-02	The organization protects the confidentiality, integrity, and availability of data-at-rest.
					CPS.PR.DS-06	The organization performs routine backups of data (e.g., component configurations and operational data), protects backup data, and tests restoration capabilities.
			b. Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI at backup storage locations.		CPS.PR.DS-02	The organization protects the confidentiality, integrity, and availability of data-at-rest.
Personnel Security	03.09.01	Personnel Screening	a. Screen individuals prior to authorizing access to the system.	PS-03 Personnel Screening	CPS.GV.RR-05	The organization incorporates security-related matters (e.g., revoking access privileges and screening employees) into measures that address role changes resulting from personnel transfers.
			b. Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening].		—	—
	03.09.02	Personnel Termination and Transfer	a. When individual employment is terminated: 1. Disable system access within [Assignment: organization-defined time period]. 2. Terminate or revoke authenticators and credentials associated with the individual, and 3. Retrieve security-related system property.	- PS-04 Personnel Termination - PS-05 Personnel Transfer	CPS.GV.RR-05	The organization incorporates security-related matters (e.g., revoking access privileges and screening employees) into measures that address role changes resulting from personnel transfers.
					CPS.PR.AA-01	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.
			b. When individuals are reassigned or transferred to other positions in the organization: 1. Review and confirm the ongoing operational need for current logical and physical access authorizations to the system and facility, and 2. Modify access authorization to correspond with any changes in operational need.		CPS.GV.RR-05	The organization incorporates security-related matters (e.g., revoking access privileges and screening employees) into measures that address role changes resulting from personnel transfers.
					CPS.PR.AA-06	The organization periodically reviews granted access privileges and remediates unnecessary or excessive permissions.
Physical Protection	03.10.01	Physical Access Authorizations	a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides.	PE-02 Physical Access Authorizations	CPS.PR.AA-07	The organization implements physical safeguards, such as locking installation areas for IoT devices, servers, and related assets, controlling entry and exit, deploying biometric authentication, installing surveillance cameras, and conducting baggage and weight inspections.
			b. Issue authorization credentials for facility access.		CPS.PR.AA-01	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.
			c. Review the facility access list [Assignment: organization-defined frequency].		CPS.PR.AA-06	The organization periodically reviews granted access privileges and remediates unnecessary or excessive permissions.
			d. Remove individuals from the facility access list when access is no longer required.		CPS.GV.RR-05	The organization incorporates security-related matters (e.g., revoking access privileges and screening employees) into measures that address role changes resulting from personnel transfers.
	03.10.02	Monitoring Physical Access	a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents.	PE-06 Monitoring Physical Access	CPS.PR.AA-07	The organization implements physical safeguards, such as locking installation areas for IoT devices, servers, and related assets, controlling entry and exit, deploying biometric authentication, installing surveillance cameras, and conducting baggage and weight inspections.
					CPS.DE.CM-05	The organization implements appropriate physical access settings, logging, and monitoring, commensurate with the criticality of IoT devices, servers, and related assets.
			b. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events].		CPS.DE.CM-05	The organization implements appropriate physical access settings, logging, and monitoring, commensurate with the criticality of IoT devices, servers, and related assets.
	03.10.03	Withdrawn	Incorporated into 03.10.07.			
	03.10.04	Withdrawn	Incorporated into 03.10.07.			
	03.10.05	Withdrawn	Incorporated into 03.10.07.			
	03.10.06	Alternate Work Site	a. Determine alternate work sites allowed for use by employees.	PE-17 Alternate Work Site	—	—
			b. Employ the following security requirements at alternate work sites: [Assignment: organization-defined security requirements].		—	—

NIST SP 800-171 (Rev.3)				NIST SP 800-53 (Rev.5 Release 5.1.1) Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework Ver 1.1	
FAMILY	ID	Category	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement
	03.10.07	Physical Access Control	a. Enforce physical access authorizations at entry and exit points to the facility where the system resides by: 1. Verifying individual physical access authorizations before granting access to the facility and 2. Controlling ingress and egress with physical access control systems, devices, or guards.	- PE-03 Physical Access Control - PE-05 Access Control for Output Devices	CPS.PR.AA-07	The organization implements physical safeguards, such as locking installation areas for IoT devices, servers, and related assets, controlling entry and exit, deploying biometric authentication, installing surveillance cameras, and conducting baggage and weight inspections.
			b. Maintain physical access audit logs for entry or exit points.		CPS.DE.CM-05	The organization implements appropriate physical access settings, logging, and monitoring, commensurate with the criticality of IoT devices, servers, and related assets.
			c. Escort visitors, and control visitor activity.		—	—
			d. Secure keys, combinations, and other physical access devices.		CPS.PR.AA-07	The organization implements physical safeguards, such as locking installation areas for IoT devices, servers, and related assets, controlling entry and exit, deploying biometric authentication, installing surveillance cameras, and conducting baggage and weight inspections.
			e. Control physical access to output devices to prevent unauthorized individuals from obtaining access to CUI.		CPS.PR.AA-07	The organization implements physical safeguards, such as locking installation areas for IoT devices, servers, and related assets, controlling entry and exit, deploying biometric authentication, installing surveillance cameras, and conducting baggage and weight inspections.
	03.10.08	Access Control for Transmission	Control physical access to system distribution and transmission lines within organizational facilities.	PE-04 Access Control for Transmission	CPS.PR.AA-07	The organization implements physical safeguards, such as locking installation areas for IoT devices, servers, and related assets, controlling entry and exit, deploying biometric authentication, installing surveillance cameras, and conducting baggage and weight inspections.
Risk Assessment	03.11.01	Risk Assessment	a. Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI.	- RA-03 Risk Assessment - RA-03(01) Risk Assessment Supply Chain Risk Assessment - SR-06 Supplier Assessments and Reviews	CPS.GV.SC-03	The organization integrates cybersecurity supply chain risk management into its cybersecurity and enterprise risk management, risk assessment, and improvement processes.
					CPS.ID.RA-03	- The organization identifies and documents potential security incidents, their impacts, and their causal factors regarding organizational assets. - From the planning and design stages of IoT devices and IoT-integrated systems, the organization verifies that no unacceptable known security risks exist, incorporating safety hazard perspectives.
					CPS.ID.RA-04	The organization identifies the potential impact and likelihood of threats exploiting vulnerabilities by periodically conducting risk assessments to evaluate the effectiveness of security rules for component management, including their implementation methods.
			b. Update risk assessments [Assignment: organization-defined frequency].		CPS.ID.RA-04	The organization identifies the potential impact and likelihood of threats exploiting vulnerabilities by periodically conducting risk assessments to evaluate the effectiveness of security rules for component management, including their implementation methods.
	03.11.02	Vulnerability Monitoring and Scanning	a. Monitor and scan the system for vulnerabilities [Assignment: organization defined frequency] and when new vulnerabilities affecting the system are identified. b. Remediate system vulnerabilities within [Assignment: organization-defined response times]. c. Update system vulnerabilities to be scanned [Assignment: organization-defined frequency] and when new vulnerabilities are identified and reported.	- RA-05 Vulnerability Monitoring and Scanning - RA-05(02) Vulnerability Monitoring and Scanning Update Vulnerabilities to be Scanned	CPS.DE.CM-06 CPS.PR.PS-08 CPS.PR.PS-09 CPS.ID.RA-02	The organization periodically scans its IoT devices, servers, and related assets to identify vulnerabilities requiring remediation. The organization develops a vulnerability remediation plan and remediates component vulnerabilities in accordance with the plan. The organization applies security-critical updates for IoT devices, servers, and related assets in a timely manner using managed tools while appropriately recording history. The organization establishes a process to collect, analyze, respond to, and utilize vulnerability and threat information from internal and external sources (e.g., internal tests, security information, and security researchers).
	03.11.03	Withdrawn	Incorporated into 03.11.02.			
	03.11.04	Risk Response	Respond to findings from security assessments, monitoring, and audits.	RA-07 Risk Response	CPS.ID.RA-06	- Based on risk assessments, the organization clearly defines response measures for potential security risks, documents the defined scope and priorities of response actions, monitors the implementation progress, and communicates this status to relevant parties. - The organization appropriately addresses security and associated safety risks identified through the assessment in the planning and design stages of IoT devices and IoT-integrated systems.

NIST SP 800-171 (Rev.3)				NIST SP 800-53 (Rev.5 Release 5.1.1) Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework Ver 1.1	
FAMILY	ID	Category	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement
Security Assessment and Monitoring	03.12.01	Security Assessment	Assess the security requirements for the system and its environment of operation [Assignment: organization-defined frequency] to determine if the requirements have been satisfied.	· CA-02 Control Assessments	CPS.GV.OV-02	The organization reviews the implementation status of its cybersecurity risk management and updates it as necessary.
					CPS.ID.RA-04	The organization identifies the potential impact and likelihood of threats exploiting vulnerabilities by periodically conducting risk assessments to evaluate the effectiveness of security rules for component management, including their implementation methods.
	03.12.02	Plan of Action and Milestones	a. Develop a plan of action and milestones for the system: 1. To document the planned remediation actions to correct weaknesses or deficiencies noted during security assessments and 2. To reduce or eliminate known system vulnerabilities.	· CA-05 Plan of Action and Milestones	CPS.ID.RA-06	- Based on risk assessments, the organization clearly defines response measures for potential security risks, documents the defined scope and priorities of response actions, monitors the implementation progress, and communicates this status to relevant parties. - The organization appropriately addresses security and associated safety risks identified through the assessment in the planning and design stages of IoT devices and IoT-integrated systems.
					CPS.PR.PS-08	The organization develops a vulnerability remediation plan and remediates component vulnerabilities in accordance with the plan.
			b. Update the existing plan of action and milestones based on the findings from: 1. Security assessments, 2. Audits or reviews, and 3. Continuous monitoring activities.		CPS.ID.IM-04	The organization continuously improves asset protection processes by integrating lessons learned from security incident response as well as from monitoring, measuring, and assessing internal and external attacks.
	03.12.03	Continuous Monitoring	Develop and implement a system-level continuous monitoring strategy that includes ongoing monitoring and security assessments.	· CA-07 Continuous Monitoring	CPS.DE.CM-01	The organization monitors networks and network services to properly detect security events.
					CPS.DE.CM-02	The organization monitors the operational status of hardware and software across IoT devices, servers, and related assets, as well as network connection status, to properly detect security events.
					CPS.DE.CM-03	The organization monitors communications with external service providers to properly detect security events.
					CPS.DE.CM-04	The organization monitors the activities of internal and external personnel, including their access to and operations on elements (components, systems, etc.), to properly detect security events.
					CPS.DE.CM-09	As part of its monitoring operations, the organization periodically tests and validates whether functions detecting security events operate as intended.
	03.12.04	Withdrawn	Incorporated into 03.15.02.			
	03.12.05	Information Exchange	a. Approve and manage the exchange of CUI between the system and other systems using [Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service-level agreements; user agreements; non-disclosure agreements; other types of agreements].	· CA-03 Information Exchange	CPS.GV.SC-05	The organization establishes supply chain cybersecurity standards considering the lifecycle of business relationships, clearly defines the scope of responsibilities, and agrees on them with partners through contracts or other means.
			b. Document interface characteristics, security requirements, and responsibilities for each system as part of the exchange agreements.		CPS.GV.SC-05	The organization establishes supply chain cybersecurity standards considering the lifecycle of business relationships, clearly defines the scope of responsibilities, and agrees on them with partners through contracts or other means.
			c. Review and update the exchange agreements [Assignment: organization-defined frequency].		—	—

NIST SP 800-171 (Rev.3)				NIST SP 800-53 (Rev.5 Release 5.1.1) Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework Ver 1.1	
FAMILY	ID	Category	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement
System and Communications Protection	03.13.01	Boundary Protection	a. Monitor and control communications at external managed interfaces to the system and key internal managed interfaces within the system.	· SC-07 Boundary Protection	CPS.DE.CM-01	The organization monitors networks and network services to properly detect security events.
					CPS.DE.CM-02	The organization monitors the operational status of hardware and software across IoT devices, servers, and related assets, as well as network connection status, to properly detect security events.
					CPS.DE.CM-03	The organization monitors communications with external service providers to properly detect security events.
			b. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.		CPS.PR.IR-01	The organization protects networks and environments from unauthorized access and use by implementing network segmentation (e.g., separating development/test environments from production environments, and isolating IoT device environments from other networks within the organization).
			c. Connect to external systems only through managed interfaces that consist of boundary protection devices arranged in accordance with an organizational security architecture.		—	—
	03.13.02	Withdrawn	Recategorized as NCO.			
	03.13.03	Withdrawn	Addressed by 03.01.01, 03.01.02, 03.01.03, 03.01.04, 03.01.05, 03.01.06, and 03.01.07.			
	03.13.04	Information in Shared System Resources	Prevent unauthorized and unintended information transfer via shared system resources.	· SC-04 Information in Shared System Resources	CPS.PR.DS-04	The organization protects the confidentiality, integrity, and availability of data-in-use.
	03.13.05	Withdrawn	Incorporated into 03.13.01.			
	03.13.06	Network Communications – Deny by Default – Allow by Exception	Deny network communications traffic by default, and allow network communications traffic by exception.	· SC-07(05) Boundary Protection Deny by Default – Allow by Exception	CPS.PR.PS-06	The organization establishes and applies configuration management practices for hardware and software of IoT devices, servers, and related assets (including minimizing functionality by physically or logically disabling unnecessary network, USB, and serial ports).
	03.13.07	Withdrawn	Addressed by 03.01.12, 03.04.02 and 03.04.06.			
	03.13.08	Transmission and Storage Confidentiality	Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI during transmission and while in storage.	· AC-17(02) Remote Access Protection of Confidentiality and Integrity Using Encryption · SC-08 Transmission Confidentiality and Integrity · SC-08(01) Transmission Confidentiality and Integrity Cryptographic Protection · SC-28 Protection of Information at Rest · SC-28(01) Protection of Information at Rest Cryptographic Protection	CPS.PR.DS-02	The organization protects the confidentiality, integrity, and availability of data-at-rest.
					CPS.PR.DS-03	The organization protects the confidentiality, integrity, and availability of data-in-transit.
	03.13.09	Network Disconnect	Terminate the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.	· SC-10 Network Disconnect	—	—
	03.13.10	Cryptographic Key Establishment and Management	Establish and manage cryptographic keys in the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].	· SC-12 Cryptographic Key Establishment and Management	CPS.PR.AA-01	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.
					CPS.PR.PS-12	Upon the disposal of IoT devices, servers, and related assets, the organization deletes or renders unreadable all internally stored data, unique identifiers of legitimate devices and systems, and critical security information (e.g., private keys and digital certificates).

NIST SP 800-171 (Rev.3)				NIST SP 800-53 (Rev.5 Release 5.1.1) Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework Ver 1.1	
FAMILY	ID	Category	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement
	03.13.11	Cryptographic Protection	Implement the following types of cryptography to protect the confidentiality of CUI: [Assignment: organization-defined types of cryptography].	· SC-13 Cryptographic Protection	CPS.PR.DS-02	The organization protects the confidentiality, integrity, and availability of data-at-rest.
					CPS.PR.DS-03	The organization protects the confidentiality, integrity, and availability of data-in-transit.
					CPS.PR.DS-04	The organization protects the confidentiality, integrity, and availability of data-in-use.
	03.13.12	Collaborative Computing Devices and Applications	a. Prohibit the remote activation of collaborative computing devices and applications with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed].	· SC-15 Collaborative Computing Devices and Applications	—	—
			b. Provide an explicit indication of use to users physically present at the devices.		—	—
	03.13.13	Mobile Code	a. Define acceptable mobile code and mobile code technologies.	· SC-18 Mobile Code	—	—
			b. Authorize, monitor, and control the use of mobile code.		CPS.DE.CM-08	The organization deploys IoT devices that detect anomalies or suspend operations by comparing commanded operations with actual operational outcomes. The organization verifies that information received from cyberspace does not contain malicious code and remains within permissible operating parameters prior to execution.
	03.13.14	Withdrawn	Technology-specific.			
	03.13.15	Session Authenticity	Protect the authenticity of communications sessions.	· SC-23 Session Authenticity	CPS.DE.CM-07	The organization verifies the integrity and authenticity of information received from cyberspace prior to operation.
	03.13.16	Withdrawn	Incorporated into 03.13.08.			
System and Information Integrity	03.14.01	Flaw Remediation	a. Identify, report, and correct system flaws.	· SI-02 Flaw Remediation	CPS.ID.RA-01	The organization identifies vulnerabilities in its assets and manages them by linking them to the corresponding assets.
					CPS.PR.PS-08	The organization develops a vulnerability remediation plan and remediates component vulnerabilities in accordance with the plan.
					CPS.DE.CM-06	The organization periodically scans its IoT devices, servers, and related assets to identify vulnerabilities requiring remediation.
			b. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates.		CPS.PR.PS-09	The organization applies security-critical updates for IoT devices, servers, and related assets in a timely manner using managed tools while appropriately recording history.
	03.14.02	Malicious Code Protection	a. Implement malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code.	· SI-03 Malicious Code Protection	CPS.DE.CM-08	The organization deploys IoT devices that detect anomalies or suspend operations by comparing commanded operations with actual operational outcomes. The organization verifies that information received from cyberspace does not contain malicious code and remains within permissible operating parameters prior to execution.
			b. Update malicious code protection mechanisms as new releases are available in accordance with configuration management policies and procedures.		CPS.PR.PS-09	The organization applies security-critical updates for IoT devices, servers, and related assets in a timely manner using managed tools while appropriately recording history.
			c. Configure malicious code protection mechanisms to: 1. Perform scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at endpoints or system entry and exit points as the files are downloaded, opened, or executed; and 2. Block malicious code, quarantine malicious code, or take other mitigation actions in response to malicious code detection.		—	—

NIST SP 800-171 (Rev.3)				NIST SP 800-53 (Rev.5 Release 5.1.1) Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework Ver 1.1	
FAMILY	ID	Category	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement
	03.14.03	Security Alerts, Advisories, and Directives	a. Receive system security alerts, advisories, and directives from external organizations on an ongoing basis.	· SI-05 Security Alerts, Advisories, and Directives	CPS.ID.RA-02	The organization establishes a process to collect, analyze, respond to, and utilize vulnerability and threat information from internal and external sources (e.g., internal tests, security information, and security researchers).
			b. Generate and disseminate internal system security alerts, advisories, and directives, as necessary.		CPS.GV.RM-06	The organization establishes and maintains lines of communication across the organization regarding cybersecurity risks, including risks posed by partners and other third parties.
	03.14.04	Withdrawn	Incorporated into 03.14.02.			
	03.14.05	Withdrawn	Addressed by 03.14.02.			
	03.14.06	System Monitoring	a. Monitor the system to detect: 1. Attacks and indicators of potential attacks and 2. Unauthorized connections.	· SI-04 System Monitoring · SI-04(04) System Monitoring Inbound and Outbound Communications Traffic	CPS.DE.CM-02	The organization monitors the operational status of hardware and software across IoT devices, servers, and related assets, as well as network connection status, to properly detect security events.
			b. Identify unauthorized use of the system.		CPS.DE.CM-04	The organization monitors the activities of internal and external personnel, including their access to and operations on elements (components, systems, etc.), to properly detect security events.
			c. Monitor inbound and outbound communications traffic to detect unusual or unauthorized activities or conditions.		CPS.DE.CM-01	The organization monitors networks and network services to properly detect security events.
	03.14.07	Withdrawn	Incorporated into 03.14.06.			
	03.14.08	Information Management and Retention	Manage and retain CUI within the system and CUI output from the system in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.	· SI-12 Information Management and Retention	—	—
					CPS.PR.DS-01	The organization accurately understands the required level of data protection mandated by various laws, regulations, and agreements regarding data shared exclusively among relevant organizations, establishes data classification methods based on respective requirements, and appropriately protects data commensurate with its classification throughout the entire lifecycle.
Planning	03.15.01	Policy and Procedures	a. Develop, document, and disseminate to organizational personnel or roles the policies and procedures needed to satisfy the security requirements for the protection of CUI.	· AC-01 Policy and Procedures · AT-01 Policy and Procedures · AU-01 Policy and Procedures · CA-01 Policy and Procedures · CM-01 Policy and Procedures · IA-01 Policy and Procedures · IR-01 Policy and Procedures · MA-01 Policy and Procedures · MP-01 Policy and Procedures · PE-01 Policy and Procedures · PL-01 Policy and Procedures · PS-01 Policy and Procedures · RA-01 Policy and Procedures · SA-01 Policy and Procedures · SC-01 Policy and Procedures · SI-01 Policy and Procedures · SR-01 Policy and Procedures	CPS.GV.PO-01	The organization formulates security policies based on its organizational context, cybersecurity strategy, and priorities, communicates them within the organization and to relevant external parties (including suppliers and third-party providers, as needed), and implements them.
			b. Review and update policies and procedures [Assignment: organization-defined frequency].		CPS.GV.PO-02	The organization periodically reviews its security policies and updates them as necessary, based on changes in requirements, threats, technology, and the organization's mission.
	03.15.02	System Security Plan	a. Develop a system security plan that: 1. Defines the constituent system components; 2. Identifies the information types processed, stored, and transmitted by the system; 3. Describes specific threats to the system that are of concern to the organization; 4. Describes the operational environment for the system and any dependencies on or connections to other systems or system components; 5. Provides an overview of the security requirements for the system; 6. Describes the safeguards in place or planned for meeting the security requirements; 7. Identifies individuals that fulfill system roles and responsibilities; and 8. Includes other relevant information necessary for the protection of CUI.	· PL-02 System Security and Privacy Plans	—	—
			b. Review and update the system security plan [Assignment: organization-defined frequency].		CPS.GV.OV-02	The organization reviews the implementation status of its cybersecurity risk management and updates it as necessary.
			c. Protect the system security plan from unauthorized disclosure.		CPS.PR.DS-02	The organization protects the confidentiality, integrity, and availability of data-at-rest.

NIST SP 800-171 (Rev.3)				NIST SP 800-53 (Rev.5 Release 5.1.1) Relevant Security Controls referred from NIST SP 800-171	Cyber/Physical Security Framework Ver 1.1	
FAMILY	ID	Category	Security Requirements	Security Controls	Measure Requirement ID	Measure Requirement
	03.15.03	Rules of Behavior	a. Establish rules that describe the responsibilities and expected behavior for system usage and protecting CUI.	· PL-04 Rules of Behavior	CPS.GV.OC-02	The organization understands legal, regulatory, and contractual requirements regarding cybersecurity—including privacy and civil liberties obligations—as well as industry guidelines, and establishes internal rules that appropriately reflect and address these requirements or guidelines.
			b. Provide rules to individuals who require access to the system.		CPS.GV.PO-01	The organization formulates security policies based on its organizational context, cybersecurity strategy, and priorities, communicates them within the organization and to relevant external parties (including suppliers and third-party providers, as needed), and implements them.
			c. Receive a documented acknowledgement from individuals indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to CUI and the system.		—	—
			d. Review and update the rules of behavior [Assignment: organization-defined frequency].		CPS.GV.PO-02	The organization periodically reviews its security policies and updates them as necessary, based on changes in requirements, threats, technology, and the organization's mission.
System and Services Acquisition	03.16.01	Security Engineering Principles	Apply the following systems security engineering principles to the development or modification of the system and system components: [Assignment: organization defined systems security engineering principles].	· SA-08 Security and Privacy Engineering Principles	CPS.PR.PS-05	The organization integrates secure software development practices (e.g., security reviews during the design stage, application of secure coding rules, and pre-release vulnerability assessments) into the system development life cycle and verifies their implementation.
	03.16.02	Unsupported System Components	a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer.	· SA-22 Unsupported System Components	CPS.ID.AM-06	The organization manages systems, hardware, software, services, and data throughout their entire lifecycle, from acquisition to disposal.
			b. Provide options for risk mitigation or alternative sources for continued support for unsupported components that cannot be replaced.		—	—
	03.16.03	External System Services	a. Require the providers of external system services used for the processing, storage, or transmission of CUI to comply with the following security requirements: [Assignment: organization-defined security requirements].	· SA-09 External System Services	CPS.GV.SC-05	The organization establishes supply chain cybersecurity standards considering the lifecycle of business relationships, clearly defines the scope of responsibilities, and agrees on them with partners through contracts or other means.
			b. Define and document user roles and responsibilities with regard to external system services, including shared responsibilities with external service providers.		CPS.GV.SC-02	The organization establishes cybersecurity roles and responsibilities for suppliers and partners, communicates them internally and externally, and coordinates adjustments as necessary.
			c. Implement processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis.		CPS.GV.SC-08	The organization periodically evaluates other relevant organizations such as business partners using audits, test results, or other forms of assessment to confirm that they are fulfilling their contractual obligations.
					CPS.GV.SC-10	The organization establishes policies and procedures for determining, based on the criticality of the technology products and services to be procured, those for which records of their sources and, to the extent reasonably ascertainable, their distribution channels are to be obtained.
	03.17.01	Supply Chain Risk Management Plan	a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services.	· SR-02 Supply Chain Risk Management Plan	CPS.GV.SC-01	The organization establishes supply chain risk management programs, strategies, objectives, policies, and processes, and operates them upon agreement with organizational stakeholders.
			b. Review and update the supply chain risk management plan [Assignment: organization-defined frequency].		CPS.GV.SC-03	The organization integrates cybersecurity supply chain risk management into its cybersecurity and enterprise risk management, risk assessment, and improvement processes.
					CPS.ID.IM-02	The organization continuously improves supply chain security standards and associated procedures.
			c. Protect the supply chain risk management plan from unauthorized disclosure.		CPS.PR.DS-02	The organization protects the confidentiality, integrity, and availability of data-at-rest.
	03.17.02	Acquisition Strategies, Tools, and Methods	Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.	· SR-05 Acquisition Strategies, Tools, and Methods	CPS.GV.SC-01	The organization establishes supply chain risk management programs, strategies, objectives, policies, and processes, and operates them upon agreement with organizational stakeholders.
	03.17.03	Supply Chain Requirements and Processes	a. Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes.	· SR-03 Supply Chain Controls and Processes	CPS.GV.SC-08	The organization periodically evaluates other relevant organizations such as business partners using audits, test results, or other forms of assessment to confirm that they are fulfilling their contractual obligations.
					CPS.GV.SC-09	The organization establishes and implements procedures to be followed when non-compliance with contractual requirements is identified through audits or testing of other relevant organizations such as business partners.
			b. Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events: [Assignment: organization-defined security requirements].		CPS.GV.SC-07	When entering into contracts with other relevant organizations such as business partners, the organization considers its objectives and risk management outcomes, verifying that products and services provided by them conform to the organization's security requirements.

D.3 Mapping ISO/IEC 27001 controls to Cyber/Physical Security Framework v1.1

ISO/IEC 27001:2022 Annex A			Cyber/Physical Security Framework Ver 1.1	
Security Controls ID		Controls	Measure Requirement ID	Measure Requirement
5 Organizational controls	5.1 Policies for information security	Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	CPS.GV.PO-01	The organization formulates security policies based on its organizational context, cybersecurity strategy, and priorities, communicates them within the organization and to relevant external parties (including suppliers and third-party providers, as needed), and implements them.
			CPS.GV.PO-02	The organization periodically reviews its security policies and updates them as necessary, based on changes in requirements, threats, technology, and the organization’s mission.
	5.2 Information security roles and responsibilities	Information security roles and responsibilities shall be defined and allocated according to the organization needs.	CPS.GV.RR-01	Organizational senior management is responsible and accountable for cybersecurity risk, fostering a culture that is risk-aware, ethical, and continually improving.
			CPS.GV.RR-02	The organization establishes roles, responsibilities, and authorities related to its cybersecurity risk management and communicates them within the organization.
			CPS.GV.RR-03	The organization appoints a security manager, establishes a security response organization (SOC/CSIRT), and maintains a structure to detect, analyze, and respond to security incidents within the organization.
			CPS.GV.SC-02	The organization establishes cybersecurity roles and responsibilities for suppliers and partners, communicates them internally and externally, and coordinates adjustments as necessary.
	5.3 Segregation of duties	Conflicting duties and conflicting areas of responsibility shall be segregated.	CPS.PR.AA-05	The organization defines rules regarding the granting of access privileges in its security policies and incorporates the principles of least privilege and separation of duties.
	5.4 Management responsibilities	Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	CPS.GV.RR-01	Organizational senior management is responsible and accountable for cybersecurity risk, fostering a culture that is risk-aware, ethical, and continually improving.
			CPS.GV.PO-01	The organization formulates security policies based on its organizational context, cybersecurity strategy, and priorities, communicates them within the organization and to relevant external parties (including suppliers and third-party providers, as needed), and implements them.
	5.5 Contact with authorities	The organization shall establish and maintain contact with relevant authorities.	CPS.RS.CO-01	The organization develops and implements rules governing internal communication and external disclosure after the occurrence of a security incident.
	5.6 Contact with special interest groups	The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	CPS.ID.RA-02	The organization establishes a process to collect, analyze, respond to, and utilize vulnerability and threat information from internal and external sources (e.g., internal tests, security information, and security researchers).
			CPS.ID.RA-05	The organization shares information regarding the effectiveness of protective technologies with appropriate partners.
	5.7 Threat intelligence	Information relating to information security threats shall be collected and analysed to produce threat intelligence.	CPS.ID.RA-02	The organization establishes a process to collect, analyze, respond to, and utilize vulnerability and threat information from internal and external sources (e.g., internal tests, security information, and security researchers).
			CPS.DE.AE-02	The organization accurately identifies security incidents by implementing procedures to correlate security events and analyze them against external threat information.
	5.8 Information security in project management	Information security shall be integrated into project management.	CPS.PR.PS-05	The organization integrates secure software development practices (e.g., security reviews during the design stage, application of secure coding rules, and pre-release vulnerability assessments) into the system development life cycle and verifies their implementation.

ISO/IEC 27001:2022 Annex A			Cyber/Physical Security Framework Ver 1.1	
Security Controls ID		Controls	Measure Requirement ID	Measure Requirement
	5.9 Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, shall be developed and maintained.	CPS.ID.AM-01	The organization develops and appropriately manages inventories of hardware, software, and their management information (e.g., name, version, network address, designated manager, and license information) that comprise its system.
			CPS.ID.AM-05	The organization develops and appropriately manages inventories of data and metadata in its possession.
	5.10 Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	CPS.GV.PO-01	The organization formulates security policies based on its organizational context, cybersecurity strategy, and priorities, communicates them within the organization and to relevant external parties (including suppliers and third-party providers, as needed), and implements them.
	5.11 Return of assets	Personnel and other interested parties as appropriate shall return all the organization’s assets in their possession upon change or termination of their employment, contract or agreement.	CPS.GV.RR-05	The organization incorporates security-related matters (e.g., revoking access privileges and screening employees) into measures that address role changes resulting from personnel transfers.
			CPS.GV.SC-11	The organization establishes and implements procedures to be followed upon the termination of contracts with partners and other parties.
	5.12 Classification of information	Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	CPS.PR.DS-01	The organization accurately understands the required level of data protection mandated by various laws, regulations, and agreements regarding data shared exclusively among relevant organizations, establishes data classification methods based on respective requirements, and appropriately protects data commensurate with its classification throughout the entire lifecycle.
			CPS.ID.AM-04	The organization categorizes and prioritizes resources (e.g., components, data, and systems) based on their function, criticality, and business value, defines management responsibilities, and communicates them to relevant organizations and people involved in their operation.
	5.13 Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	CPS.PR.DS-01	The organization accurately understands the required level of data protection mandated by various laws, regulations, and agreements regarding data shared exclusively among relevant organizations, establishes data classification methods based on respective requirements, and appropriately protects data commensurate with its classification throughout the entire lifecycle.
	5.14 Information transfer	Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.	CPS.PR.DS-03	The organization protects the confidentiality, integrity, and availability of data-in-transit.
	5.15 Access control	Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.	CPS.PR.AA-05	The organization defines rules regarding the granting of access privileges in its security policies and incorporates the principles of least privilege and separation of duties.
	5.16 Identity management	The full life cycle of identities shall be managed.	CPS.PR.AA-01	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.
	5.17 Authentication information	Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.	CPS.PR.AA-01	The organization establishes and implements procedures to issue, manage, verify, revoke, and audit identities and credentials for authorized components, people, and procedures.
	5.18 Access rights	Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	CPS.PR.AA-06	The organization periodically reviews granted access privileges and remediates unnecessary or excessive permissions.
	5.19 Information security in supplier relationships	Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	CPS.GV.SC-01	The organization establishes supply chain risk management programs, strategies, objectives, policies, and processes, and operates them upon agreement with organizational stakeholders.
	5.20 Addressing information security within supplier agreements	Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	CPS.GV.SC-05	The organization establishes supply chain cybersecurity standards considering the lifecycle of business relationships, clearly defines the scope of responsibilities, and agrees on them with partners through contracts or other means.

ISO/IEC 27001:2022 Annex A			Cyber/Physical Security Framework Ver 1.1	
Security Controls ID		Controls	Measure Requirement ID	Measure Requirement
	5.21 Managing information security in the information and communication technology (ICT) supply chain	Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	CPS.GV.SC-01	The organization establishes supply chain risk management programs, strategies, objectives, policies, and processes, and operates them upon agreement with organizational stakeholders.
	5.22 Monitoring, review and change management of supplier services	The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	CPS.GV.SC-08	The organization periodically evaluates other relevant organizations such as business partners using audits, test results, or other forms of assessment to confirm that they are fulfilling their contractual obligations.
			CPS.GV.SC-09	The organization establishes and implements procedures to be followed when non-compliance with contractual requirements is identified through audits or testing of other relevant organizations such as business partners.
			CPS.GV.SC-10	The organization establishes policies and procedures for determining, based on the criticality of the technology products and services to be procured, those for which records of their sources and, to the extent reasonably ascertainable, their distribution channels are to be obtained.
	5.23 Information security for use of cloud services	Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.	CPS.GV.SC-05	The organization establishes supply chain cybersecurity standards considering the lifecycle of business relationships, clearly defines the scope of responsibilities, and agrees on them with partners through contracts or other means.
	5.24 Information security incident management planning and preparation	The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	CPS.GV.RR-03	The organization appoints a security manager, establishes a security response organization (SOC/CSIRT), and maintains a structure to detect, analyze, and respond to security incidents within the organization.
			CPS.RS.MA-01	To clarify response actions, priorities, and remediation scope following the occurrence of a security incident, the organization predefines and implements response procedures (security operation processes) for the organization, people, components, and systems after detecting an incident.
	5.25 Assessment and decision on information security events	The organization shall assess information security events and decide if they are to be categorized as information security incidents.	CPS.DE.AE-01	The organization analyzes potential security events to understand their details.
			CPS.DE.AE-04	The organization establishes criteria for determining whether a security event constitutes an incident, and declares an incident when the criteria are met.
			CPS.RS.MA-02	The organization verifies that events reported as security incidents are not false positives or duplicate reports, and validates their legitimacy as incidents.
	5.26 Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	CPS.RS.MA-04	Once a security incident is declared, the organization executes incident response in accordance with predefined procedures, coordinating with other relevant organizations such as business partners.
	5.27 Learning from information security incidents	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	CPS.ID.IM-04	The organization continuously improves asset protection processes by integrating lessons learned from security incident response as well as from monitoring, measuring, and assessing internal and external attacks.
			CPS.ID.IM-06	The organization incorporates lessons learned from responses to security incidents to continuously improve its incident response plan.
	5.28 Collection of evidence	The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	CPS.RS.AN-01	The organization collects data and metadata related to security incidents (including the history of actions taken during incident response), preserves their integrity, and retains them in a state where acquisition sources, timestamps, and related provenance can be referenced.

ISO/IEC 27001:2022 Annex A			Cyber/Physical Security Framework Ver 1.1	
Security Controls ID		Controls	Measure Requirement ID	Measure Requirement
			CPS.RS.AN-02	After a security incident occurs, the organization conducts digital forensics to identify the root cause. In doing so, it preserves records of the investigation process in a tamper-resistant manner.
	5.29 Information security during disruption	The organization shall plan how to maintain information security at an appropriate level during disruption.	CPS.RC.RP-01	The organization incorporates security incidents into its business continuity plan or emergency response plan, which defines response policies and procedures for natural disasters.
	5.30 ICT readiness for business continuity	ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	CPS.PR.IR-03	The organization implements mechanisms to achieve requirements for the continuous operation of systems and services under normal and adverse conditions.
			CPS.PR.IR-04	The organization secures sufficient resources (e.g., people, components, and systems) to minimize the impact of attacks and maintain critical functions, even in the event of cyberattacks such as ransomware or denial-of-service (DoS) attacks.
	5.31 Legal, statutory, regulatory and contractual requirements	Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.	CPS.GV.OC-02	The organization understands legal, regulatory, and contractual requirements regarding cybersecurity—including privacy and civil liberties obligations—as well as industry guidelines, and establishes internal rules that appropriately reflect and address these requirements or guidelines.
	5.32 Intellectual property rights	The organization shall implement appropriate procedures to protect intellectual property rights.	—	—
	5.33 Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	CPS.PR.DS-02	The organization protects the confidentiality, integrity, and availability of data-at-rest.
	5.34 Privacy and protection of personal identifiable information (PII)	The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	CPS.GV.OC-02	The organization understands legal, regulatory, and contractual requirements regarding cybersecurity—including privacy and civil liberties obligations—as well as industry guidelines, and establishes internal rules that appropriately reflect and address these requirements or guidelines.
	5.35 Independent review of information security	The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.	CPS.GV.OV-02	The organization reviews the implementation status of its cybersecurity risk management and updates it as necessary.
	5.36 Compliance with policies, rules and standards for information security	Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.	CPS.GV.OV-02	The organization reviews the implementation status of its cybersecurity risk management and updates it as necessary.
	5.37 Documented operating procedures	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	—	—
6 People controls	6.1 Screening	Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	CPS.GV.RR-05	The organization incorporates security-related matters (e.g., revoking access privileges and screening employees) into measures that address role changes resulting from personnel transfers.
	6.2 Terms and conditions of employment	The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	—	—
	6.3 Information security awareness, education and training	Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	CPS.PR.AT-01	The organization conducts appropriate training and education for all personnel to carry out their assigned roles and responsibilities to minimize the occurrence and impact of security incidents, and maintains records of such activities.
			CPS.PR.AT-02	The organization provides appropriate training and security education to designated personnel of external partners critical to security management, who may be involved in security incident response for the organization, enabling them to fulfill their assigned roles, and maintains records of such activities.
	6.4 Disciplinary process	A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	—	—
	6.5 Responsibilities after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.	CPS.GV.RR-05	The organization incorporates security-related matters (e.g., revoking access privileges and screening employees) into measures that address role changes resulting from personnel transfers.

ISO/IEC 27001:2022 Annex A			Cyber/Physical Security Framework Ver 1.1	
Security Controls ID		Controls	Measure Requirement ID	Measure Requirement
	6.6 Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	—	—
	6.7 Remote working	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	—	—
	6.8 Information security event reporting	The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	CPS.GV.RR-03	The organization appoints a security manager, establishes a security response organization (SOC/CSIRT), and maintains a structure to detect, analyze, and respond to security incidents within the organization.
			CPS.GV.RM-06	The organization establishes and maintains lines of communication across the organization regarding cybersecurity risks, including risks posed by partners and other third parties.
7 Physical controls	7.1 Physical security perimeters	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	—	—
	7.2 Physical entry	Secure areas shall be protected by appropriate entry controls and access points.	CPS.PR.AA-07	The organization implements physical safeguards, such as locking installation areas for IoT devices, servers, and related assets, controlling entry and exit, deploying biometric authentication, installing surveillance cameras, and conducting baggage and weight inspections.
	7.3 Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and implemented.	CPS.PR.AA-07	The organization implements physical safeguards, such as locking installation areas for IoT devices, servers, and related assets, controlling entry and exit, deploying biometric authentication, installing surveillance cameras, and conducting baggage and weight inspections.
	7.4 Physical security monitoring	Premises shall be continuously monitored for unauthorized physical access.	CPS.DE.CM-05	The organization implements appropriate physical access settings, logging, and monitoring, commensurate with the criticality of IoT devices, servers, and related assets.
	7.5 Protecting against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.	CPS.PR.IR-02	The organization implements physical safeguards to comply with policies and rules regarding the physical operating environment of its IoT devices, servers, and related assets, such as ensuring uninterruptible power supplies, fire protection equipment, and flood protection measures.
	7.6 Working in secure areas	Security measures for working in secure areas shall be designed and implemented.	CPS.PR.AA-07	The organization implements physical safeguards, such as locking installation areas for IoT devices, servers, and related assets, controlling entry and exit, deploying biometric authentication, installing surveillance cameras, and conducting baggage and weight inspections.
	7.7 Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	CPS.PR.AA-07	The organization implements physical safeguards, such as locking installation areas for IoT devices, servers, and related assets, controlling entry and exit, deploying biometric authentication, installing surveillance cameras, and conducting baggage and weight inspections.
	7.8 Equipment siting and protection	Equipment shall be sited securely and protected.	CPS.PR.AA-07	The organization implements physical safeguards, such as locking installation areas for IoT devices, servers, and related assets, controlling entry and exit, deploying biometric authentication, installing surveillance cameras, and conducting baggage and weight inspections.
			CPS.PR.IR-02	The organization implements physical safeguards to comply with policies and rules regarding the physical operating environment of its IoT devices, servers, and related assets, such as ensuring uninterruptible power supplies, fire protection equipment, and flood protection measures.
	7.9 Security of assets off-premises	Off-site assets shall be protected.	CPS.ID.AM-06	The organization manages systems, hardware, software, services, and data throughout their entire lifecycle, from acquisition to disposal.
	7.10 Storage media	Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	CPS.ID.AM-06	The organization manages systems, hardware, software, services, and data throughout their entire lifecycle, from acquisition to disposal.
	7.11 Supporting utilities	Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	CPS.PR.IR-02	The organization implements physical safeguards to comply with policies and rules regarding the physical operating environment of its IoT devices, servers, and related assets, such as ensuring uninterruptible power supplies, fire protection equipment, and flood protection measures.
	7.12 Cabling security	Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.	CPS.PR.IR-02	The organization implements physical safeguards to comply with policies and rules regarding the physical operating environment of its IoT devices, servers, and related assets, such as ensuring uninterruptible power supplies, fire protection equipment, and flood protection measures.

ISO/IEC 27001:2022 Annex A			Cyber/Physical Security Framework Ver 1.1	
Security Controls ID		Controls	Measure Requirement ID	Measure Requirement
	7.13 Equipment maintenance	Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	CPS.PR.PS-10	The organization performs maintenance on its own IoT devices, servers, and related assets with prior approval from the department that owns the target component or system, logging maintenance activities and preventing unauthorized access.
	7.14 Secure disposal or re-use of equipment	Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	CPS.PR.PS-12	Upon the disposal of IoT devices, servers, and related assets, the organization deletes or renders unreadable all internally stored data, unique identifiers of legitimate devices and systems, and critical security information (e.g., private keys and digital certificates).
8 Technological controls	8.1 User end point devices	Information stored on, processed by or accessible via user end point devices shall be protected.	CPS.PR.DS-02	The organization protects the confidentiality, integrity, and availability of data-at-rest.
			CPS.PR.DS-04	The organization protects the confidentiality, integrity, and availability of data-in-use.
	8.2 Privileged access rights	The allocation and use of privileged access rights shall be restricted and managed.	CPS.PR.AA-05	The organization defines rules regarding the granting of access privileges in its security policies and incorporates the principles of least privilege and separation of duties.
			CPS.PR.AA-06	The organization periodically reviews granted access privileges and remediates unnecessary or excessive permissions.
	8.3 Information access restriction	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	CPS.PR.AA-02	The organization authenticates and authorizes logical access to components (physical items, systems, etc.) by IoT devices and users using highly reliable methods (e.g., multi-factor authentication) commensurate with transaction risks (personal security, privacy risks, and other organizational risks).
	8.4 Access to source code	Read and write access to source code, development tools and software libraries shall be appropriately managed.	CPS.PR.AA-02	The organization authenticates and authorizes logical access to components (physical items, systems, etc.) by IoT devices and users using highly reliable methods (e.g., multi-factor authentication) commensurate with transaction risks (personal security, privacy risks, and other organizational risks).
	8.5 Secure authentication	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.	CPS.PR.AA-02	The organization authenticates and authorizes logical access to components (physical items, systems, etc.) by IoT devices and users using highly reliable methods (e.g., multi-factor authentication) commensurate with transaction risks (personal security, privacy risks, and other organizational risks).
			CPS.PR.AA-03	The organization prevents unauthorized logins to IoT devices, servers, and related assets by implementing mechanisms such as account lockout after a specified number of failed authentication attempts and enforcing delays on subsequent login attempts until security conditions are verified.
	8.6 Capacity management	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	CPS.PR.IR-04	The organization secures sufficient resources (e.g., people, components, and systems) to minimize the impact of attacks and maintain critical functions, even in the event of cyberattacks such as ransomware or denial-of-service (DoS) attacks.
	8.7 Protection against malware	Protection against malware shall be implemented and supported by appropriate user awareness.	CPS.PR.PS-01	The organization evaluates the authenticity and integrity of hardware and software prior to acquisition and deployment, and verifies their integrity during operation.
			CPS.PR.PS-07	The organization prevents the installation and execution of unauthorized software.
			CPS.DE.CM-07	The organization verifies the integrity and authenticity of information received from cyberspace prior to operation.
			CPS.DE.CM-08	The organization deploys IoT devices that detect anomalies or suspend operations by comparing commanded operations with actual operational outcomes. The organization verifies that information received from cyberspace does not contain malicious code and remains within permissible operating parameters prior to execution.

ISO/IEC 27001:2022 Annex A			Cyber/Physical Security Framework Ver 1.1	
Security Controls ID		Controls	Measure Requirement ID	Measure Requirement
	8.8 Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use shall be obtained, the organization’s exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	CPS.ID.RA-01	The organization identifies vulnerabilities in its assets and manages them by linking them to the corresponding assets.
			CPS.DE.CM-06	The organization periodically scans its IoT devices, servers, and related assets to identify vulnerabilities requiring remediation.
			CPS.PR.PS-08	The organization develops a vulnerability remediation plan and remediates component vulnerabilities in accordance with the plan.
	8.9 Configuration management	Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	CPS.PR.PS-06	The organization establishes and applies configuration management practices for hardware and software of IoT devices, servers, and related assets (including minimizing functionality by physically or logically disabling unnecessary network, USB, and serial ports).
	8.10 Information deletion	Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	CPS.PR.PS-12	Upon the disposal of IoT devices, servers, and related assets, the organization deletes or renders unreadable all internally stored data, unique identifiers of legitimate devices and systems, and critical security information (e.g., private keys and digital certificates).
	8.11 Data masking	Data masking shall be used in accordance with the organization’s topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	CPS.PR.DS-01	The organization accurately understands the required level of data protection mandated by various laws, regulations, and agreements regarding data shared exclusively among relevant organizations, establishes data classification methods based on respective requirements, and appropriately protects data commensurate with its classification throughout the entire lifecycle.
	8.12 Data leakage prevention	Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	CPS.PR.DS-02	The organization protects the confidentiality, integrity, and availability of data-at-rest.
			CPS.PR.DS-03	The organization protects the confidentiality, integrity, and availability of data-in-transit.
			CPS.PR.DS-04	The organization protects the confidentiality, integrity, and availability of data-in-use.
	8.13 Information backup	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	CPS.PR.DS-06	The organization performs routine backups of data (e.g., component configurations and operational data), protects backup data, and tests restoration capabilities.
	8.14 Redundancy of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	CPS.PR.IR-03	The organization implements mechanisms to achieve requirements for the continuous operation of systems and services under normal and adverse conditions.
			CPS.PR.IR-04	The organization secures sufficient resources (e.g., people, components, and systems) to minimize the impact of attacks and maintain critical functions, even in the event of cyberattacks such as ransomware or denial-of-service (DoS) attacks.
	8.15 Logging	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.	CPS.PR.PS-11	To appropriately detect security incidents, the organization determines and documents the scope and types of events for audit logging, and continuously records and reviews logs.
			CPS.DE.AE-01	The organization analyzes potential security events to understand their details.

ISO/IEC 27001:2022 Annex A			Cyber/Physical Security Framework Ver 1.1	
Security Controls ID		Controls	Measure Requirement ID	Measure Requirement
	8.16 Monitoring activities	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	CPS.DE.CM-01	The organization monitors networks and network services to properly detect security events.
			CPS.DE.CM-02	The organization monitors the operational status of hardware and software across IoT devices, servers, and related assets, as well as network connection status, to properly detect security events.
			CPS.DE.CM-03	The organization monitors communications with external service providers to properly detect security events.
			CPS.DE.CM-04	The organization monitors the activities of internal and external personnel, including their access to and operations on elements (components, systems, etc.), to properly detect security events.
	8.17 Clock synchronization	The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	—	—
	8.18 Use of privileged utility programs	The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.	—	—
	8.19 Installation of software on operational systems	Procedures and measures shall be implemented to securely manage software installation on operational systems.	CPS.PR.PS-01	The organization evaluates the authenticity and integrity of hardware and software prior to acquisition and deployment, and verifies their integrity during operation.
			CPS.PR.PS-07	The organization prevents the installation and execution of unauthorized software.
	8.20 Networks security	Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.	CPS.PR.IR-01	The organization protects networks and environments from unauthorized access and use by implementing network segmentation (e.g., separating development/test environments from production environments, and isolating IoT device environments from other networks within the organization).
	8.21 Security of network services	Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	CPS.DE.CM-01	The organization monitors networks and network services to properly detect security events.
	8.22 Segregation of networks	Groups of information services, users and information systems shall be segregated in the organization's networks.	CPS.PR.IR-01	The organization protects networks and environments from unauthorized access and use by implementing network segmentation (e.g., separating development/test environments from production environments, and isolating IoT device environments from other networks within the organization).
	8.23 Web filtering	Access to external websites shall be managed to reduce exposure to malicious content.	—	—

ISO/IEC 27001:2022 Annex A			Cyber/Physical Security Framework Ver 1.1	
Security Controls ID		Controls	Measure Requirement ID	Measure Requirement
	8.24 Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	CPS.PR.DS-02	The organization protects the confidentiality, integrity, and availability of data-at-rest.
			CPS.PR.DS-03	The organization protects the confidentiality, integrity, and availability of data-in-transit.
			CPS.PR.DS-04	The organization protects the confidentiality, integrity, and availability of data-in-use.
	8.25 Secure development life cycle	Rules for the secure development of software and systems shall be established and applied.	CPS.PR.PS-05	The organization integrates secure software development practices (e.g., security reviews during the design stage, application of secure coding rules, and pre-release vulnerability assessments) into the system development life cycle and verifies their implementation.
	8.26 Application security requirements	Information security requirements shall be identified, specified and approved when developing or acquiring applications.	CPS.PR.PS-05	The organization integrates secure software development practices (e.g., security reviews during the design stage, application of secure coding rules, and pre-release vulnerability assessments) into the system development life cycle and verifies their implementation.
	8.27 Secure system architecture and engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.	CPS.PR.PS-05	The organization integrates secure software development practices (e.g., security reviews during the design stage, application of secure coding rules, and pre-release vulnerability assessments) into the system development life cycle and verifies their implementation.
	8.28 Secure coding	Secure coding principles shall be applied to software development.	CPS.PR.PS-05	The organization integrates secure software development practices (e.g., security reviews during the design stage, application of secure coding rules, and pre-release vulnerability assessments) into the system development life cycle and verifies their implementation.
	8.29 Security testing in development and acceptance	Security testing processes shall be defined and implemented in the development life cycle.	CPS.PR.PS-05	The organization integrates secure software development practices (e.g., security reviews during the design stage, application of secure coding rules, and pre-release vulnerability assessments) into the system development life cycle and verifies their implementation.
	8.30 Outsourced development	The organization shall direct, monitor and review the activities related to outsourced system development.	—	—
	8.31 Separation of development, test and production environments	Development, testing and production environments shall be separated and secured.	CPS.PR.IR-01	The organization protects networks and environments from unauthorized access and use by implementing network segmentation (e.g., separating development/test environments from production environments, and isolating IoT device environments from other networks within the organization).
	8.32 Change management	Changes to information processing facilities and information systems shall be subject to change management procedures.	CPS.PR.PS-06	The organization establishes and applies configuration management practices for hardware and software of IoT devices, servers, and related assets (including minimizing functionality by physically or logically disabling unnecessary network, USB, and serial ports).
	8.33 Test information	Test information shall be appropriately selected, protected and managed.	CPS.PR.DS-02	The organization protects the confidentiality, integrity, and availability of data-at-rest.
	8.34 Protection of information systems during audit testing	Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.	—	—