

**NIST IR 8477-Based Set Theory Relationship Mapping (STRM)**

**Reference document:** Security Controls Framework (SCF) version 2026.1  
**STRM document:** <https://securecontrolsframework.com/start-here-set-theory-relationship-mapping-strm/>

**Focal Document:**  
**Published STRM URL:**

**Cloud Security Alliance (CSA) Internet of Things Security Controls Framework v2**  
<https://cloudsecurityalliance.org/artifacts/csa-iot-security-controls-framework-v2/>  
<https://content.securecontrolsframework.com/strm/scf-strm-general-csa-iot-2.pdf>

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Security Controls Framework (SCF) Control Description	Strength of Relationship	Notes
ASM-01	N/A	Schedule a task to update the asset/inventory database at least quarterly.	Functional	Subset Of	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	10	
ASM-02	N/A	Deploy an inventory management system and record details about each IoT device in inventory. Use this inventory management system to track each IoT device's version, including firmware and patch status, real-time operating systems (RTOS) version/image version, application/library versions, lost or decommissioned status, and to whom the device is assigned. Include device location.	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
ASM-03	N/A	Monitor IoT node power levels by configuring nodes to alert regarding low battery or increased battery drainage. Investigate any discovered incidents associated with excess battery drainage.	Functional	Subset Of	Power Level Monitoring	EMB-09	Automated mechanisms exist to monitor the power levels of embedded technologies for decreased or excessive power usage, including battery drainage, to investigate for device tampering.	10	
ASM-04	N/A	Establish naming conventions for IoT devices and configure unique identifiers to each device. Identifiers should be unique across the enterprise and designed in a manner that allows for the incorporation of large quantities of additional devices (e.g., mergers/acquisitions) at a later time without name conflicts.	Functional	Subset Of	Standardized Naming Convention	AST-01.3	Mechanisms exist to implement a scalable, standardized naming convention for Technology Assets, Applications, Services and/or Data (TAASD) that avoids asset naming conflicts.	10	
CCM-01	N/A	Evaluate legacy IoT devices annually for technology upgrades. In the interim, use gateway security mechanisms to extend the security boundary and mitigate risks exposed by these legacy devices.	Functional	Intersects With	Embedded Technology Reviews	EMB-10	Mechanisms exist to perform evaluations of deployed embedded technologies as needed, or at least on an annual basis, to ensure that necessary updates to mitigate the risks associated with legacy embedded technologies are identified and implemented.	8	
CCM-01	N/A	Evaluate legacy IoT devices annually for technology upgrades. In the interim, use gateway security mechanisms to extend the security boundary and mitigate risks exposed by these legacy devices.	Functional	Subset Of	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	10	
CCM-02	N/A	Define and follow a quality change control and testing process (e.g., information technology infrastructure library (ITIL) service management) with established baselines, testing, and release standards that focus on system availability, confidentiality, and integrity of systems and services.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
CCM-02	N/A	Define and follow a quality change control and testing process (e.g., information technology infrastructure library (ITIL) service management) with established baselines, testing, and release standards that focus on system availability, confidentiality, and integrity of systems and services.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	8	
CCM-02	N/A	Define and follow a quality change control and testing process (e.g., information technology infrastructure library (ITIL) service management) with established baselines, testing, and release standards that focus on system availability, confidentiality, and integrity of systems and services.	Functional	Intersects With	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	8	
CCM-03	N/A	Implement a configuration management program that detects all modifications to IoT system configuration files. Implement response plans upon the detection of unauthorized changes.	Functional	Intersects With	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	8	
CCM-03	N/A	Implement a configuration management program that detects all modifications to IoT system configuration files. Implement response plans upon the detection of unauthorized changes.	Functional	Intersects With	Configuration Enforcement	CFG-06	Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices.	8	
CCM-03	N/A	Implement a configuration management program that detects all modifications to IoT system configuration files. Implement response plans upon the detection of unauthorized changes.	Functional	Intersects With	Embedded Technology Configuration Monitoring	EMB-05	Mechanisms exist to generate log entries on embedded devices when configuration changes or attempts to access interfaces are detected.	8	
CCM-05	N/A	Review IoT inventories annually to identify products used within the enterprise that have reached or will reach end-of-life within the next year. This review should include checks to ensure the vendor has not announced plans to discontinue support for the products or their associated services. Flag any device at risk of end-of-life and take action to procure updated devices.	Functional	Subset Of	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	10	
CCM-06	N/A	Implement a secure staging system for over-the-air updates to protect from intrusion and malicious logic. Apply integrity controls to files before transmitting them to edge devices.	Functional	Intersects With	Segregation From Enterprise Services	NET-06.4	Mechanisms exist to isolate sensitive/regulatory data enclaves (secure zones) from corporate-provided IT resources by providing enclave-specific IT services (e.g., directory services, DNS, NTP, ITAM, antimalware, patch management, etc.) to those isolated network segments.	8	
CCM-06	N/A	Implement a secure staging system for over-the-air updates to protect from intrusion and malicious logic. Apply integrity controls to files before transmitting them to edge devices.	Functional	Intersects With	Software & Firmware Integrity Verification	TDA-14.1	Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of software and firmware components.	5	
CCM-06	N/A	Implement a secure staging system for over-the-air updates to protect from intrusion and malicious logic. Apply integrity controls to files before transmitting them to edge devices.	Functional	Intersects With	Centralized Management of Flow Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flow remediation process.	8	
CCM-07	N/A	Integrity protect firmware images of IoT devices. Define processes to restore IoT devices should those devices be suspected compromised or corrupted. Test update processes at least annually across different device types.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	8	
CCM-07	N/A	Integrity protect firmware images of IoT devices. Define processes to restore IoT devices should those devices be suspected compromised or corrupted. Test update processes at least annually across different device types.	Functional	Intersects With	Centralized Management of Flow Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flow remediation process.	8	
CCM-07	N/A	Integrity protect firmware images of IoT devices. Define processes to restore IoT devices should those devices be suspected compromised or corrupted. Test update processes at least annually across different device types.	Functional	Intersects With	Automated Software & Firmware Updates	VPM-05.4	Automated mechanisms exist to install the latest stable versions of security-relevant software and firmware updates.	8	
CCM-08	N/A	Establish a configuration control board (CCB) to vet modifications/changes to IoT systems. A CCB should define processes for updates, including testing (functional, security, interoperability) of all updates before fielding.	Functional	Intersects With	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	8	
CCM-08	N/A	Establish a configuration control board (CCB) to vet modifications/changes to IoT systems. A CCB should define processes for updates, including testing (functional, security, interoperability) of all updates before fielding.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	8	
CCM-08	N/A	Establish a configuration control board (CCB) to vet modifications/changes to IoT systems. A CCB should define processes for updates, including testing (functional, security, interoperability) of all updates before fielding.	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	8	
CCM-08	N/A	Establish a configuration control board (CCB) to vet modifications/changes to IoT systems. A CCB should define processes for updates, including testing (functional, security, interoperability) of all updates before fielding.	Functional	Intersects With	Security, Compliance & Resilience Representative for Asset Lifecycle Changes	CHG-02.3	Mechanisms exist to include a cybersecurity and/or data protection representative in the configuration change control review process.	8	
CCM-08	N/A	Establish a configuration control board (CCB) to vet modifications/changes to IoT systems. A CCB should define processes for updates, including testing (functional, security, interoperability) of all updates before fielding.	Functional	Intersects With	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	8	
CLS-01	N/A	Provision digital certificates to all cloud servers, services, and gateways to establish trusted communication.	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5	
CLS-01	N/A	Provision digital certificates to all cloud servers, services, and gateways to establish trusted communication.	Functional	Intersects With	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.	8	
CLS-01	N/A	Provision digital certificates to all cloud servers, services, and gateways to establish trusted communication.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
CLS-01	N/A	Provision digital certificates to all cloud servers, services, and gateways to establish trusted communication.	Functional	Intersects With	Public Key Infrastructure (PKI)	CRY-08	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	8	
CLS-01	N/A	Provision digital certificates to all cloud servers, services, and gateways to establish trusted communication.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	8	
CLS-01	N/A	Provision digital certificates to all cloud servers, services, and gateways to establish trusted communication.	Functional	Intersects With	PKI-Based Authentication	IAC-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	8	
CLS-02	N/A	Configure cloud gateways to accept communications from only trusted devices. Whitelist authorized devices and log attempted communications from unauthorized devices.	Functional	Intersects With	Side Channel Attack Prevention	CLD-12	Mechanisms exist to prevent "side channel attacks" when using a Content Delivery Network (CDN) by restricting access to the origin server's IP address to the CDN and an authorized management network.	5	
CLS-02	N/A	Configure cloud gateways to accept communications from only trusted devices. Whitelist authorized devices and log attempted communications from unauthorized devices.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	8	
CLS-04	N/A	Establish a privacy agreement with your cloud service provider (CSP). Ensure appropriate security controls are in place for protection of sensitive data (personally identifiable information (PII)/protected health information (PHI)).	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	8	
CLS-04	N/A	Establish a privacy agreement with your cloud service provider (CSP). Ensure appropriate security controls are in place for protection of sensitive data (personally identifiable information (PII)/protected health information (PHI)).	Functional	Intersects With	Adequate Security for Sensitive / Regulated Data in Support of Contracts	IAD-03.2	Mechanisms exist to protect sensitive/regulatory data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	8	
CLS-04	N/A	Establish a privacy agreement with your cloud service provider (CSP). Ensure appropriate security controls are in place for protection of sensitive data (personally identifiable information (PII)/protected health information (PHI)).	Functional	Subset Of	Data Privacy Requirements for Contractors & Service Providers	PRR-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	10	
CLS-04	N/A	Establish a privacy agreement with your cloud service provider (CSP). Ensure appropriate security controls are in place for protection of sensitive data (personally identifiable information (PII)/protected health information (PHI)).	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	8	
CLS-05	N/A	Configure cloud services securely.	Functional	Subset Of	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10	
CLS-05	N/A	Configure cloud services securely.	Functional	Intersects With	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.	8	
CLS-05	N/A	Configure cloud services securely.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
CLS-05	N/A	Configure cloud services securely.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
CLS-05	N/A	Configure cloud services securely.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	8	
CLS-05	N/A	Configure cloud services securely.	Functional	Intersects With	Centralized Management of Security, Compliance & Resilience Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of security, compliance and resilience controls and related processes.	8	
CLS-06	N/A	Keep all cloud infrastructure updated and patched.	Functional	Subset Of	Vulnerability & Patch Management Program (VPM)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
CLS-06	N/A	Keep all cloud infrastructure updated and patched.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	8	
CLS-06	N/A	Keep all cloud infrastructure updated and patched.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	8	
CLS-06	N/A	Keep all cloud infrastructure updated and patched.	Functional	Intersects With	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	8	
CLS-06	N/A	Keep all cloud infrastructure updated and patched.	Functional	Intersects With	Stable Versions	VPM-04.1	Mechanisms exist to install the latest stable version of any software and/or security-related updates on all applicable systems.	8	
CLS-06	N/A	Keep all cloud infrastructure updated and patched.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	8	
CLS-06	N/A	Keep all cloud infrastructure updated and patched.	Functional	Intersects With	Centralized Management of Flow Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flow remediation process.	8	
CLS-06	N/A	Keep all cloud infrastructure updated and patched.	Functional	Intersects With	Automated Software & Firmware Updates	VPM-05.4	Automated mechanisms exist to install the latest stable versions of security-relevant software and firmware updates.	8	
CLS-07	N/A	Monitor all application programming interface (API) calls and alert for potential API misuse.	Functional	Intersects With	Application Programming Interface (API) Security	CLD-04	Mechanisms exist to ensure support for secure interoperability between components with Application Programming Interfaces (APIs).	5	
CLS-07	N/A	Monitor all application programming interface (API) calls and alert for potential API misuse.	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	8	
CLS-07	N/A	Monitor all application programming interface (API) calls and alert for potential API misuse.	Functional	Intersects With	Analyze and Prioritize Monitoring Requirements	MON-01.16	Mechanisms exist to assess the organization's needs for monitoring and prioritize the monitoring of Technology Assets, Applications and/or Services (TAAS), based on TAAS criticality and the sensitivity of the data it stores, transmits and processes.	8	
CLS-08	N/A	Authenticate IoT devices to cloud services. Deny access to any device that fails authentication and log that access attempt, and set thresholds for the number of failures in a time period that triggers an alert to security administrators.	Functional	Intersects With	Restrict Communications	EMB-12	Mechanisms exist to require embedded technologies to initiate all communications and drop new, incoming communications.	5	
CLS-08	N/A	Authenticate IoT devices to cloud services. Deny access to any device that fails authentication and log that access attempt, and set thresholds for the number of failures in a time period that triggers an alert to security administrators.	Functional	Intersects With	Authorized Communications	EMB-13	Mechanisms exist to restrict embedded technologies to communicate only with authorized peers and service endpoints.	5	
CLS-08	N/A	Authenticate IoT devices to cloud services. Deny access to any device that fails authentication and log that access attempt, and set thresholds for the number of failures in a time period that triggers an alert to security administrators.	Functional	Intersects With	Certificate-Based Authentication	EMB-16	Mechanisms exist to enforce certificate-based authentication for embedded technologies (e.g., IoT, OT, etc.) and their supporting services.	5	
CLS-08	N/A	Authenticate IoT devices to cloud services. Deny access to any device that fails authentication and log that access attempt, and set thresholds for the number of failures in a time period that triggers an alert to security administrators.	Functional	Intersects With	Chip-To-Cloud Security	EMB-17	Mechanisms exist to implement embedded technologies that utilize pre-provisioned cloud trust anchors to support secure bootstrap and Zero Touch Provisioning (ZTP).	5	
CLS-08	N/A	Authenticate IoT devices to cloud services. Deny access to any device that fails authentication and log that access attempt, and set thresholds for the number of failures in a time period that triggers an alert to security administrators.	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	5	
CLS-08	N/A	Authenticate IoT devices to cloud services. Deny access to any device that fails authentication and log that access attempt, and set thresholds for the number of failures in a time period that triggers an alert to security administrators.	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
CLS-09	N/A	Require authentication to IoT service management consoles. Provision unique identities for each operator and administrator with access to the management console.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	8	
CLS-11	N/A	Enforce multi-factor authentication for management console login to cloud services.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data.	8	
CLS-12	N/A	Restrict the scope of all cloud APIs to specific internet protocol (IP) addresses, gateways or applications.	Functional	Intersects With	Application Programming Interface (API) Security	CLD-04	Mechanisms exist to ensure support for secure interoperability between components with Application Programming Interfaces (APIs).	5	
CLS-12	N/A	Restrict the scope of all cloud APIs to specific internet protocol (IP) addresses, gateways or applications.	Functional	Intersects With	Cloud Access Security Broker (CASB)	CLD-11	Mechanisms exist to utilize a Cloud Access Security Broker (CASB), or similar technology, to provide boundary protection and monitoring functions that both provide access to the cloud and protect the organization from misuse of cloud resources.	3	
CLS-12	N/A	Restrict the scope of all cloud APIs to specific internet protocol (IP) addresses, gateways or applications.	Functional	Intersects With	Side Channel Attack Prevention	CLD-12	Mechanisms exist to prevent "side channel attacks" when using a Content Delivery Network (CDN) by restricting access to the origin server's IP address to the CDN and an authorized management network.	3	
CLS-12	N/A	Restrict the scope of all cloud APIs to specific internet protocol (IP) addresses, gateways or applications.	Functional	Intersects With	Data Flow Enforcement - Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	8	
CLS-12	N/A	Restrict the scope of all cloud APIs to specific internet protocol (IP) addresses, gateways or applications.	Functional	Intersects With	Refresh from Trusted Sources	SEA-08.1	Mechanisms exist to ensure that software and data needed for system component and service refreshes are obtained from trusted sources.	8	
CLS-13	N/A	Restrict the allowable operations of each API (e.g., read-only, read/write, etc.)	Functional	Intersects With	Application Programming Interface (API) Security	CLD-04	Mechanisms exist to ensure support for secure interoperability between components with Application Programming Interfaces (APIs).	8	
CLS-14	N/A	Protect hosts used to remotely access cloud management consoles from malware infection using anti-virus protections and host-based security monitoring.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimicrobial technologies to detect and eradicate malicious code.	8	
CLS-14	N/A	Protect hosts used to remotely access cloud management consoles from malware infection using anti-virus protections and host-based security monitoring.	Functional	Intersects With	Host Intrusion Detection and Prevention Systems (HIDS / HIPS)	END-07	Mechanisms exist to utilize Host-based Intrusion Detection / Prevention Systems (HIDS / HIPS), or similar technologies, to monitor for and protect against anomalous host activity, including lateral movement across the network.	3	
COM-01	N/A	Enforce security for message queuing telemetry transport (MQTT) protocol messaging. Define authorized MQTT topics and create/enforce an access control list within the broker to restrict IoT devices from publishing content or subscribing to unauthorized message topics. Encrypt all MQTT messages. Use certificates to authenticate MQTT transactions. Consider throttling traffic to MQTT servers on both a global and per-client basis and always route MQTT traffic through a firewall. Reduce the standard MQTT message size to limit an attacker's ability to overload the system by sending large messages.	Functional	Subset Of	Message Queuing Telemetry Transport (MQTT) Security	EMB-11	Mechanisms exist to enforce the security of Message Queuing Telemetry Transport (MQTT) traffic.	10	
COM-07	N/A	Encrypt all transmission control protocol (TCP)-based communications (e.g., representational state transfer (REST), MQTT, advanced message queuing protocol (AMQP)) between system components using X.509 authenticated transport layer security (TLS).	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	8	
COM-07	N/A	Encrypt all transmission control protocol (TCP)-based communications (e.g., representational state transfer (REST), MQTT, advanced message queuing protocol (AMQP)) between system components using X.509 authenticated transport layer security (TLS).	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	8	
COM-07	N/A	Encrypt all transmission control protocol (TCP)-based communications (e.g., representational state transfer (REST), MQTT, advanced message queuing protocol (AMQP)) between system components using X.509 authenticated transport layer security (TLS).	Functional	Intersects With	Message Queuing Telemetry Transport (MQTT) Security	EMB-11	Mechanisms exist to enforce the security of Message Queuing Telemetry Transport (MQTT) traffic.	8	
COM-08	N/A	Encrypt all user datagram protocol (UDP)-based communications (e.g., constrained application protocol (CoAP) between system components using the datagram transport layer security (DTLS) protocol specified in Internet Engineering Task Force (IETF) Request for Comments (RFC) 7525 or newer).	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	8	
COM-08	N/A	Encrypt all user datagram protocol (UDP)-based communications (e.g., constrained application protocol (CoAP) between system components using the datagram transport layer security (DTLS) protocol specified in Internet Engineering Task Force (IETF) Request for Comments (RFC) 7525 or newer).	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	8	
COM-09	N/A	Enforce end-to-end authenticated encryption protocols across all IoT system endpoints. Use transport layer security (TLS) and datagram transport layer security (DTLS) as appropriate based on TCP/UDP communications. Ensure that all encryption operations align with policy guidance from the latest version of the National Institute of Standards and Technology (NIST) SP 800-131A.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	8	
COM-09	N/A	Enforce end-to-end authenticated encryption protocols across all IoT system endpoints. Use transport layer security (TLS) and datagram transport layer security (DTLS) as appropriate based on TCP/UDP communications. Ensure that all encryption operations align with policy guidance from the latest version of the National Institute of Standards and Technology (NIST) SP 800-131A.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	8	
COM-10	N/A	Configure IoT devices to drop new incoming communication attempts. Require that IoT devices initiate all communications.	Functional	Equal	Restrict Communications	EMB-12	Mechanisms exist to require embedded technologies to initiate all communications and drop new, incoming communications.	10	
COM-11	N/A	Configure IoT devices, gateways, services and applications to communicate only with authorized peers and service endpoints.	Functional	Equal	Authorized Communications	EMB-13	Mechanisms exist to restrict embedded technologies to communicate only with authorized peers and service endpoints.	10	
DAT-01	N/A	Document data collected, processed, and stored within IoT systems. Classify that data based on data type, value (criticality to the organization, and sensitivity). Label the data with tags (metadata) that can be used to identify data types flowing within the system.	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	8	
DAT-01	N/A	Document data collected, processed, and stored within IoT systems. Classify that data based on data type, value (criticality to the organization, and sensitivity). Label the data with tags (metadata) that can be used to identify data types flowing within the system.	Functional	Intersects With	Cybersecurity & Data Protection Attributes	DCH-05	Mechanisms exist to bind cybersecurity and data protection attributes to information as it is stored, transmitted and processed.	5	
DAT-01	N/A	Document data collected, processed, and stored within IoT systems. Classify that data based on data type, value (criticality to the organization, and sensitivity). Label the data with tags (metadata) that can be used to identify data types flowing within the system.	Functional	Intersects With	Metadata	NET-04.5	Mechanisms exist to enforce information flow controls based on metadata.	5	
DAT-02	N/A	Implement data security controls based on the classification of each data type	Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
DAT-03	N/A	Catalog data sources (both internal and third-party use) and enforce data authentication relied upon by the IoT system. Track the data lineage throughout the system as data is cleaned, reduced, modified, and aggregated. Then, pinpoint data sources—and any users or processes—that have acted upon any data used within an automated IoT decision process.	Functional	Intersects With	Provenance	AST-03.2	Mechanisms exist to track the origin, development, ownership, location and changes to Technology Assets, Applications, Services and/or Data (TAASD).	8	
DAT-03	N/A	Catalog data sources (both internal and third-party use) and enforce data authentication relied upon by the IoT system. Track the data lineage throughout the system as data is cleaned, reduced, modified, and aggregated. Then, pinpoint data sources—and any users or processes—that have acted upon any data used within an automated IoT decision process.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulatory data flows.	5	
DAT-03	N/A	Catalog data sources (both internal and third-party use) and enforce data authentication relied upon by the IoT system. Track the data lineage throughout the system as data is cleaned, reduced, modified, and aggregated. Then, pinpoint data sources—and any users or processes—that have acted upon any data used within an automated IoT decision process.	Functional	Intersects With	Refresh from Trusted Sources	SEA-08.1	Mechanisms exist to ensure that software and data needed for system component and service refreshes are obtained from trusted sources.	3	
DAT-04	N/A	After cataloging data within an IoT system, identify any locations and systems which store that data and apply data-at-rest encryption controls to those locations and systems. Monitor to ensure new systems and components are not implemented without evaluating their storage of sensitive information.	Functional	Intersects With	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	3	
DAT-04	N/A	After cataloging data within an IoT system, identify any locations and systems which store that data and apply data-at-rest encryption controls to those locations and systems. Monitor to ensure new systems and components are not implemented without evaluating their storage of sensitive information.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
DAT-04	N/A	After cataloging data within an IoT system, identify any locations and systems which store that data and apply data-at-rest encryption controls to those locations and systems. Monitor to ensure new systems and components are not implemented without evaluating their storage of sensitive information.	Functional	Intersects With	Geographic Location of Data	DCH-19	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physical and virtual), infrastructure, systems components and/or shared with other third-parties.	8	
GVN-01	N/A	Create a governance framework for the IoT system. Clarify the individuals responsible for distributed systems' security and their interconnection to the cloud and other data services. Require the identification of executive leadership accountable for each system and define the responsibilities of those charged with securing those systems. Identify and document the roles and responsibilities of employees and third-party users for data and assets protection within IoT systems.	Functional	Intersects With	Security, Compliance & Resilience Program (SCRIP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	8	
GVN-01	N/A	Create a governance framework for the IoT system. Clarify the individuals responsible for distributed systems' security and their interconnection to the cloud and other data services. Require the identification of executive leadership accountable for each system and define the responsibilities of those charged with securing those systems. Identify and document the roles and responsibilities of employees and third-party users for data and assets protection within IoT systems.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8	
GVN-01	N/A	Create a governance framework for the IoT system. Clarify the individuals responsible for distributed systems' security and their interconnection to the cloud and other data services. Require the identification of executive leadership accountable for each system and define the responsibilities of those charged with securing those systems. Identify and document the roles and responsibilities of employees and third-party users for data and assets protection within IoT systems.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRIP).	8	
GVN-01	N/A	Create a governance framework for the IoT system. Clarify the individuals responsible for distributed systems' security and their interconnection to the cloud and other data services. Require the identification of executive leadership accountable for each system and define the responsibilities of those charged with securing those systems. Identify and document the roles and responsibilities of employees and third-party users for data and assets protection within IoT systems.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for managing, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
GVN-01	N/A	Create a governance framework for the IoT system. Clarify the individuals responsible for distributed systems' security and their interconnection to the cloud and other data services. Require the identification of executive leadership accountable for each system and define the responsibilities of those charged with securing those systems. Identify and document the roles and responsibilities of employees and third-party users for data and assets protection within IoT systems.	Functional	Intersects With	Embedded Technology Security Program	EMB-01	Mechanisms exist to facilitate the implementation of embedded technology controls.	8	
GVN-01	N/A	Create a governance framework for the IoT system. Clarify the individuals responsible for distributed systems' security and their interconnection to the cloud and other data services. Require the identification of executive leadership accountable for each system and define the responsibilities of those charged with securing those systems. Identify and document the roles and responsibilities of employees and third-party users for data and assets protection within IoT systems.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	
GVN-02	N/A	Establish an enterprise IoT security architecture that documents the standards, regulatory, legal, and statutory requirements that must be adhered to by IoT systems within the enterprise.	Functional	Intersects With	Security, Compliance & Resilience Program (SCRIP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	8	
GVN-02	N/A	Establish an enterprise IoT security architecture that documents the standards, regulatory, legal, and statutory requirements that must be adhered to by IoT systems within the enterprise.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8	
GVN-02	N/A	Establish an enterprise IoT security architecture that documents the standards, regulatory, legal, and statutory requirements that must be adhered to by IoT systems within the enterprise.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	8	
GVN-02	N/A	Establish an enterprise IoT security architecture that documents the standards, regulatory, legal, and statutory requirements that must be adhered to by IoT systems within the enterprise.	Functional	Intersects With	Embedded Technology Security Program	EMB-01	Mechanisms exist to facilitate the implementation of embedded technology controls.	8	
GVN-02	N/A	Establish an enterprise IoT security architecture that documents the standards, regulatory, legal, and statutory requirements that must be adhered to by IoT systems within the enterprise.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	8	
GVN-02	N/A	Establish an enterprise IoT security architecture that documents the standards, regulatory, legal, and statutory requirements that must be adhered to by IoT systems within the enterprise.	Functional	Intersects With	Centralized Management of Security, Compliance & Resilience Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of security, compliance and resilience controls and related processes.	5	
GVN-02	N/A	Establish an enterprise IoT security architecture that documents the standards, regulatory, legal, and statutory requirements that must be adhered to by IoT systems within the enterprise.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	5	
GVN-03	N/A	A unified framework business continuity plan shall be created, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for backup, recovery, testing, maintenance, and information security requirements.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
GVN-04	N/A	Establish and implement an organizational compliance management program for all IoT systems. This system should be reviewed annually and used to monitor nonconformities with established policies, standards, procedures, and compliance obligations.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	8	
GVN-04	N/A	Establish and implement an organizational compliance management program for all IoT systems. This system should be reviewed annually and used to monitor nonconformities with established policies, standards, procedures, and compliance obligations.	Functional	Intersects With	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	8	
GVN-04	N/A	Establish and implement an organizational compliance management program for all IoT systems. This system should be reviewed annually and used to monitor nonconformities with established policies, standards, procedures, and compliance obligations.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	8	
GVN-04	N/A	Establish and implement an organizational compliance management program for all IoT systems. This system should be reviewed annually and used to monitor nonconformities with established policies, standards, procedures, and compliance obligations.	Functional	Intersects With	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	5	
GVN-04	N/A	Establish and implement an organizational compliance management program for all IoT systems. This system should be reviewed annually and used to monitor nonconformities with established policies, standards, procedures, and compliance obligations.	Functional	Intersects With	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	8	
GVN-04	N/A	Establish and implement an organizational compliance management program for all IoT systems. This system should be reviewed annually and used to monitor nonconformities with established policies, standards, procedures, and compliance obligations.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5	
GVN-05	N/A	Implement and enforce technical and policy mechanisms to restrict administrator ability to track location or other sensitive attributes of system users. Implement access controls and logging procedures to prevent insiders from disabling these controls without proper event logging.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	8	
GVN-05	N/A	Implement and enforce technical and policy mechanisms to restrict administrator ability to track location or other sensitive attributes of system users. Implement access controls and logging procedures to prevent insiders from disabling these controls without proper event logging.	Functional	Intersects With	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	8	
GVN-05	N/A	Implement and enforce technical and policy mechanisms to restrict administrator ability to track location or other sensitive attributes of system users. Implement access controls and logging procedures to prevent insiders from disabling these controls without proper event logging.	Functional	Intersects With	Automated Security Response	CHG-02.4	Automated mechanisms exist to implement remediation actions upon the detection of unauthorized baseline configurations changes).	5	
GVN-05	N/A	Implement and enforce technical and policy mechanisms to restrict administrator ability to track location or other sensitive attributes of system users. Implement access controls and logging procedures to prevent insiders from disabling these controls without proper event logging.	Functional	Intersects With	De-identification (Anonymization)	DCH-23	Mechanisms exist to anonymize data by removing Personal Data (PD) from datasets.	5	
GVN-05	N/A	Implement and enforce technical and policy mechanisms to restrict administrator ability to track location or other sensitive attributes of system users. Implement access controls and logging procedures to prevent insiders from disabling these controls without proper event logging.	Functional	Intersects With	Embedded Technology Configuration Monitoring	EMB-05	Mechanisms exist to generate log entries on embedded devices when configuration changes or attempts to access interfaces are detected.	8	
GVN-06	N/A	Document the metadata generated by the IoT system. Classify the metadata based on sensitivity level and identify any instances where aggregated data would increase the data sensitivity level. Establish procedures to ensure that metadata breaches are identified and handled in accordance with the organization's incident handling procedures and any applicable breach notification requirements.	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
GVN-06	N/A	Document the metadata generated by the IoT system. Classify the metadata based on sensitivity level and identify any instances where aggregated data would increase the data sensitivity level. Establish procedures to ensure that metadata breaches are identified and handled in accordance with the organization's incident handling procedures and any applicable breach notification requirements.	Functional	Intersects With	Highest Classification Level	DCH-02.1	Mechanisms exist to ensure that Technology Assets, Applications and/or Services (TAAS) are classified according to the highest level of data sensitivity that is stored, transmitted and/or processed.	8	
GVN-06	N/A	Document the metadata generated by the IoT system. Classify the metadata based on sensitivity level and identify any instances where aggregated data would increase the data sensitivity level. Establish procedures to ensure that metadata breaches are identified and handled in accordance with the organization's incident handling procedures and any applicable breach notification requirements.	Functional	Intersects With	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	5	
GVN-06	N/A	Document the metadata generated by the IoT system. Classify the metadata based on sensitivity level and identify any instances where aggregated data would increase the data sensitivity level. Establish procedures to ensure that metadata breaches are identified and handled in accordance with the organization's incident handling procedures and any applicable breach notification requirements.	Functional	Intersects With	Metadata	NET-04.5	Mechanisms exist to enforce information flow controls based on metadata.	5	
GVN-07	N/A	Require a privacy impact assessment (PIA) at the onset of any new system implementation. Systems may be internal or external facing. The PIA should address the following, at a minimum: identification of sensitive data stored on the device; mechanisms used to inform users of data collected; consent for data collection; processes for use and review of personal data before it is transferred; notice concerning data collection timing and frequency; and the ability for users to opt-in or out of data sharing.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
GVN-08	N/A	Update privacy impact assessment annually. Communicate key findings of the PIA to all system administrators supporting the operational system. Track compliance with PIA results on a continuous basis.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
GVN-09	N/A	Evaluate the safety impacts of an IoT system. Log all safety risks, prioritize the risks, and implement mitigations for each risk. Incorporate device and environmental controls to enforce safety requirements as necessary.	Functional	Intersects With	Operating Environment Certification	EMB-14	Mechanisms exist to determine if embedded technologies are certified for secure use in the proposed operating environment.	3	
GVN-09	N/A	Evaluate the safety impacts of an IoT system. Log all safety risks, prioritize the risks, and implement mitigations for each risk. Incorporate device and environmental controls to enforce safety requirements as necessary.	Functional	Intersects With	Safety Assessment	EMB-15	Mechanisms exist to evaluate the safety aspects of embedded technologies via a fault tree analysis, or similar method, to determine possible consequences of misuse, misconfiguration and/or failure.	8	
GVN-10	N/A	Conduct fault tree analysis to identify and prioritize safety risks associated with the IoT system.	Functional	Intersects With	Safety Assessment	EMB-15	Mechanisms exist to evaluate the safety aspects of embedded technologies via a fault tree analysis, or similar method, to determine possible consequences of misuse, misconfiguration and/or failure.	8	
IAM-01	N/A	Implement attribute-based access control (ABAC) to enable policy-driven dynamic authorizations within the IoT system and support secure sharing of information across the organization and partner organizations.	Functional	Subset Of	Attribute-Based Access Control (ABAC)	IAC-29	Mechanisms exist to enforce Attribute-Based Access Control (ABAC) for policy-driven, dynamic authorizations that supports the secure sharing of information.	10	
IAM-02	N/A	Audit user, administrator, service, and device accounts within the IoT system at least annually. Take action to disable any accounts that are determined unnecessary—including those that are unauthorized and expired.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	8	
IAM-02	N/A	Audit user, administrator, service, and device accounts within the IoT system at least annually. Take action to disable any accounts that are determined unnecessary—including those that are unauthorized and expired.	Functional	Intersects With	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	8	
IAM-03	N/A	Configure certificate-based authentication on IoT devices, gateways and services.	Functional	Intersects With	Certificate-Based Authentication	EMB-16	Mechanisms exist to enforce certificate-based authentication for embedded technologies (e.g., IoT, OT, etc.) and their supporting services.	8	
IAM-04	N/A	Minimize privileged service operations. Do not run network services such as web servers with root privileges. Instead, require "run as/sudo" operations. Implement and assign privileged roles to system components and users, such as trusted devices, privileged local users, system administrators, trusted applications, and trusted gateway.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	8	
IAM-04	N/A	Minimize privileged service operations. Do not run network services such as web servers with root privileges. Instead, require "run as/sudo" operations. Implement and assign privileged roles to system components and users, such as trusted devices, privileged local users, system administrators, trusted applications, and trusted gateway.	Functional	Intersects With	Use of Privileged Utility Programs	IAC-20.3	Mechanisms exist to restrict and tightly control utility programs that are capable of overriding system and application controls.	5	
IAM-04	N/A	Minimize privileged service operations. Do not run network services such as web servers with root privileges. Instead, require "run as/sudo" operations. Implement and assign privileged roles to system components and users, such as trusted devices, privileged local users, system administrators, trusted applications, and trusted gateway.	Functional	Intersects With	Non-Privileged Access for Non-Security Functions	IAC-21.2	Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions.	8	
IAM-05	N/A	For mobile IoT devices, implement geofencing restrictions to monitor or control device location to collect location data for authorization decisions.	Functional	Intersects With	Mobile Device Geofencing	MDM-09	Mechanisms exist to restrict the functionality of mobile devices based on geographic location.	8	
IAM-06	N/A	Enforce the concept of least privilege. Limit applications and services that run with elevated access, such as administrative privileges. Require authentication for all access and sensitive actions.	Functional	Subset Of	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	10	
IAM-07	N/A	Establish a process for securely bootstrapping IoT devices onto networks. Give preference to IoT devices capable of zero-touch provisioning, as these devices come pre-loaded with manufacturer credentials embedded in the hardware. Zero-touch provisioning requires a trusted out-of-band process for loading serial numbers and public keys of devices to be provisioned.	Functional	Subset Of	Zero-Touch Provisioning (ZTP)	CFG-07	Mechanisms exist to implement Zero-Touch Provisioning (ZTP), or similar technology, to automatically and securely configure devices upon being added to a network.	10	
IAM-08	N/A	Establish monitoring rules for misbehavior and procedures to revoke certificates whenever a system resource or user is suspected of being compromised.	Functional	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on indicators of compromise (IOC).	8	
IAM-08	N/A	Establish monitoring rules for misbehavior and procedures to revoke certificates whenever a system resource or user is suspected of being compromised.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	8	
IAM-08	N/A	Establish monitoring rules for misbehavior and procedures to revoke certificates whenever a system resource or user is suspected of being compromised.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
IAM-08	N/A	Establish monitoring rules for misbehavior and procedures to revoke certificates whenever a system resource or user is suspected of being compromised.	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	
IAM-08	N/A	Establish monitoring rules for misbehavior and procedures to revoke certificates whenever a system resource or user is suspected of being compromised.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: 1) Preparation; 2) Automated event detection or manual incident report intake; 3) Analysis; 4) Containment; 5) Eradication; and 6) Recovery.	5	
IAM-08	N/A	Establish monitoring rules for misbehavior and procedures to revoke certificates whenever a system resource or user is suspected of being compromised.	Functional	Intersects With	Automated Incident Handling Processes	IRO-02.1	Automated mechanisms exist to support the incident handling process.	5	
IAM-08	N/A	Establish monitoring rules for misbehavior and procedures to revoke certificates whenever a system resource or user is suspected of being compromised.	Functional	Intersects With	Automatic Disabling of Technology Assets, Applications and/or Services (TAAS)	IRO-02.6	Mechanisms exist to automatically disable Technology Assets, Applications and/or Services (TAAS), upon detection of a possible incident that meets organizational criteria, which allows for forensic analysis to be performed.	8	
IAM-09	N/A	Define misuse patterns and establish policies for revocation of credentials. Implement procedures for the submission of misbehavior reports and a process (misbehavior authority) to adjudicate reports of misbehavior. Establish and implement procedures for revocation to occur within one day of authorization.	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover: 1) Preparation; 2) Automated event detection or manual incident report intake; 3) Analysis; 4) Containment; 5) Eradication; and 6) Recovery.	10	
IAM-09	N/A	Define misuse patterns and establish policies for revocation of credentials. Implement procedures for the submission of misbehavior reports and a process (misbehavior authority) to adjudicate reports of misbehavior. Establish and implement procedures for revocation to occur within one day of authorization.	Functional	Intersects With	Indicators of Compromise (IOC)	IRO-03	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	8	
IAM-09	N/A	Define misuse patterns and establish policies for revocation of credentials. Implement procedures for the submission of misbehavior reports and a process (misbehavior authority) to adjudicate reports of misbehavior. Establish and implement procedures for revocation to occur within one day of authorization.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	8	
IAM-10	N/A	Establish operational certificate lifetimes of no more than three years. Manufacturers may embed device identity certificates with no expiration, but these certificates should only be used to establish shorter-term operational certificates.	Functional	Intersects With	Public Key Infrastructure (PKI)	CRY-08	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	5	
IAM-10	N/A	Establish operational certificate lifetimes of no more than three years. Manufacturers may embed device identity certificates with no expiration, but these certificates should only be used to establish shorter-term operational certificates.	Functional	Subset Of	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	10	
IAM-10	N/A	Establish operational certificate lifetimes of no more than three years. Manufacturers may embed device identity certificates with no expiration, but these certificates should only be used to establish shorter-term operational certificates.	Functional	Intersects With	Cryptographic Key Loss or Change	CRY-09.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	5	
IAM-11	N/A	Establish a process for certificate revocation that includes required reporting channels, investigation methods, and authorities for approving/disapproving placement on the revocation list.	Functional	Subset Of	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	10	
IAM-11	N/A	Establish a process for certificate revocation that includes required reporting channels, investigation methods, and authorities for approving/disapproving placement on the revocation list.	Functional	Intersects With	Cryptographic Key Loss or Change	CRY-09.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	5	
IAM-12	N/A	Establish certificate management policies. Define minimum requirements for validation of device identities (enrollment) before certificate provisioning.	Functional	Subset Of	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	10	
IAM-13	N/A	Establish automated certificate processes to include certificates' renewal.	Functional	Subset Of	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	10	
IAM-13	N/A	Establish automated certificate processes to include certificates' renewal.	Functional	Intersects With	Cryptographic Key Loss or Change	CRY-09.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	8	
IAM-14	N/A	Establish secure key management processes for IoT systems that include (at a minimum) key generation, key derivation, key establishment/transport, key storage, key lifetimes, and key zeroization/destruction. Keys should be generated on the devices they will be used with whenever possible, assuming those devices have a sufficiently random entropy source.	Functional	Subset Of	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
IAM-15	N/A	Establish a policy to never share private keys across multiple devices or groups and incorporate forward-secrecy whenever possible for key derivations (e.g., do not use static mechanisms). Keys should always be stored in a secure element (either software or hardware) capable of restricting key access by unauthorized actors. Keys should be limited in lifetime (when possible) to no more than three years, and ideally one year.	Functional	Subset Of	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	10	
IAM-16	N/A	Establish a specialized key management user group to securely configure key management within IoT devices and services.	Functional	Subset Of	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	10	
IAM-16	N/A	Establish a specialized key management user group to securely configure key management within IoT devices and services.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	
IAM-16	N/A	Establish a specialized key management user group to securely configure key management within IoT devices and services.	Functional	Intersects With	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
IAM-17	N/A	Document an identity management policy for the IoT system. Define appropriate uses for symmetric keys, passwords, and certificates. Restrict the provision of duplicate identity credentials (keys, certificates, passwords) to more than one device, user, or service.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
IAM-17	N/A	Document an identity management policy for the IoT system. Define appropriate uses for symmetric keys, passwords, and certificates. Restrict the provision of duplicate identity credentials (keys, certificates, passwords) to more than one device, user, or service.	Functional	Intersects With	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically-based and replay resistant.	8	
IAM-18	N/A	Enforce minimum password complexity requirements for all IoT devices and associated services (e.g., cloud services). Enforce password aging requirements. Define and enforce lock-out policies.	Functional	Subset Of	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	10	
IAM-18	N/A	Enforce minimum password complexity requirements for all IoT devices and associated services (e.g., cloud services). Enforce password aging requirements. Define and enforce lock-out policies.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	8	
IAM-19	N/A	Establish robust password processes across devices and IoT infrastructure. Do not hardcode passwords, credentials, or private keys into the device firmware. Do not provision duplicate identities or passwords across multiple devices or product lines. Follow industry standards such as NIST Special Publication 800-63: Digital Identity Guidelines.	Functional	Subset Of	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	10	
IAM-20	N/A	Review and identify devices that contain default passwords and change those passwords immediately (preferably before connecting to a network). Identify passwords shared across multiple devices and change those passwords immediately to unique values.	Functional	Subset Of	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	10	
IAM-21	N/A	If passwords are used for remote access to IoT devices, update them at least once per year. When possible, implement mechanisms that allow for the update of passwords automatically. Given the amount of IoT devices that populate networks, it is preferable to use certificates for remote access as passwords become challenging to manage as quantities of devices increase.	Functional	Subset Of	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	10	
IAM-21	N/A	If passwords are used for remote access to IoT devices, update them at least once per year. When possible, implement mechanisms that allow for the update of passwords automatically. Given the amount of IoT devices that populate networks, it is preferable to use certificates for remote access as passwords become challenging to manage as quantities of devices increase.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	8	
IAM-22	N/A	Establish a process and acquire technology to manage secure updates of devices and service trust anchors. Restrict access to updating device trust anchors to only authorized administrators.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
IAM-22	N/A	Establish a process and acquire technology to manage secure updates of devices and service trust anchors. Restrict access to updating device trust anchors to only authorized administrators.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	8	
IAM-22	N/A	Establish a process and acquire technology to manage secure updates of devices and service trust anchors. Restrict access to updating device trust anchors to only authorized administrators.	Functional	Intersects With	Cryptographic Module Authentication	IAC-12	Mechanisms exist to ensure cryptographic modules adhere to applicable statutory, regulatory and contractual requirements for security strength.	8	
IMT-01	N/A	Establish an IoT incident management plan. Identify businesses and technical points of contact (PoCs) for each IoT system and inform these stakeholders of their roles and responsibilities should an incident occur. Define the roles of third-party organizations in an incident response (e.g., vendors and service providers). Define chain-of-custody for log/audit data captured from devices. Establish escalation procedures and define forensics activities that must be performed on devices. Consider acquiring automated forensics capabilities in real-time from networked devices.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
IMT-01	N/A	Establish an IoT incident management plan. Identify businesses and technical points of contact (PoCs) for each IoT system and inform these stakeholders of their roles and responsibilities should an incident occur. Define the roles of third-party organizations in an incident response (e.g., vendors and service providers). Define chain-of-custody for log/audit data captured from devices. Establish escalation procedures and define forensics activities that must be performed on devices. Consider acquiring automated forensics capabilities in real-time from networked devices.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	8	
IMT-01	N/A	Establish an IoT incident management plan. Identify businesses and technical points of contact (PoCs) for each IoT system and inform these stakeholders of their roles and responsibilities should an incident occur. Define the roles of third-party organizations in an incident response (e.g., vendors and service providers). Define chain-of-custody for log/audit data captured from devices. Establish escalation procedures and define forensics activities that must be performed on devices. Consider acquiring automated forensics capabilities in real-time from networked devices.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	8	
IMT-01	N/A	Establish an IoT incident management plan. Identify businesses and technical points of contact (PoCs) for each IoT system and inform these stakeholders of their roles and responsibilities should an incident occur. Define the roles of third-party organizations in an incident response (e.g., vendors and service providers). Define chain-of-custody for log/audit data captured from devices. Establish escalation procedures and define forensics activities that must be performed on devices. Consider acquiring automated forensics capabilities in real-time from networked devices.	Functional	Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	5	
IMT-01	N/A	Establish an IoT incident management plan. Identify businesses and technical points of contact (PoCs) for each IoT system and inform these stakeholders of their roles and responsibilities should an incident occur. Define the roles of third-party organizations in an incident response (e.g., vendors and service providers). Define chain-of-custody for log/audit data captured from devices. Establish escalation procedures and define forensics activities that must be performed on devices. Consider acquiring automated forensics capabilities in real-time from networked devices.	Functional	Intersects With	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	5	
IMT-01	N/A	Establish an IoT incident management plan. Identify businesses and technical points of contact (PoCs) for each IoT system and inform these stakeholders of their roles and responsibilities should an incident occur. Define the roles of third-party organizations in an incident response (e.g., vendors and service providers). Define chain-of-custody for log/audit data captured from devices. Establish escalation procedures and define forensics activities that must be performed on devices. Consider acquiring automated forensics capabilities in real-time from networked devices.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	3	
IMT-01	N/A	Establish an IoT incident management plan. Identify businesses and technical points of contact (PoCs) for each IoT system and inform these stakeholders of their roles and responsibilities should an incident occur. Define the roles of third-party organizations in an incident response (e.g., vendors and service providers). Define chain-of-custody for log/audit data captured from devices. Establish escalation procedures and define forensics activities that must be performed on devices. Consider acquiring automated forensics capabilities in real-time from networked devices.	Functional	Intersects With	Third-Party Incident Response & Recovery Capabilities	TPM-11	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	3	
IOT-01	N/A	Acquire IoT products that have undergone testing and received a device security certification.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
IOT-01	N/A	Acquire IoT products that have undergone testing and received a device security certification.	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; and/or (11) Artificial Intelligence and Autonomous Technologies (AAT).	8	
IOT-01	N/A	Acquire IoT products that have undergone testing and received a device security certification.	Functional	Intersects With	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical security, compliance and resilience controls.	8	
IOT-01	N/A	Acquire IoT products that have undergone testing and received a device security certification.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	8	
IOT-02	N/A	Eliminate or lockdown unnecessary hardware features of IoT devices (e.g., unneeded radios or universal serial bus (USB) interfaces). Disable or password-protect any test interfaces (joint test action group (JTAG), universal asynchronous receiver-transmitter (UART), or general-purpose input/output (GPIO)).	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
IOT-02	N/A	Eliminate or lockdown unnecessary hardware features of IoT devices (e.g., unneeded radios or universal serial bus (USB) interfaces). Disable or password-protect any test interfaces (joint test action group (JTAG), universal asynchronous receiver-transmitter (UART), or general-purpose input/output (GPIO)).	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	8	
IOT-03	N/A	Deploy devices that validate the software signature on firmware and its components before updating.	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
IOT-03	N/A	Deploy devices that validate the software signature on firmware and its components before updating.	Functional	Intersects With	Integrity Checks	END-06.1	Mechanisms exist to validate configurations through integrity checking of software and firmware.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
IOT-04	N/A	Integrate chip-to-cloud capabilities that leverage microcontroller units (MCUs) with pre-provisioned cloud trust anchors to support more secure bootstrap and zero-touch provisioning of IoT devices. Use secure MCU hardware features to protect key material and cryptographic primitives and perform trusted bootloading by validating software before booting.	Functional	Subset Of	Chip-To-Cloud Security	EMB-17	Mechanisms exist to implement embedded technologies that utilize pre-provisioned cloud trust anchors to support secure bootstrap and Zero Touch Provisioning (ZTP).	10	
IOT-05	N/A	Deploy IoT devices that apply tamper protection for security-critical device components. Tamper protections range from simple seals and/or locked covers to piezo-electric circuits (depending on the threat environment).	Functional	Subset Of	Logical Tampering Protection	AST-15	Mechanisms exist to assess the integrity of critical Technology Assets, Applications and/or Services (TAAS) to detect evidence of tampering, where: 1) Logical assessments evaluate the integrity of critical components (e.g. configuration settings); and 2) Physical assessments evaluate assets for evidence of unauthorized access and/or modifications.	10	
IOT-05	N/A	Deploy IoT devices that apply tamper protection for security-critical device components. Tamper protections range from simple seals and/or locked covers to piezo-electric circuits (depending on the threat environment).	Functional	Intersects With	Interface Security	EMB-04	Mechanisms exist to protect embedded devices against unauthorized use of the physical factory diagnostic and test interfaces.	8	
IOT-05	N/A	Deploy IoT devices that apply tamper protection for security-critical device components. Tamper protections range from simple seals and/or locked covers to piezo-electric circuits (depending on the threat environment).	Functional	Intersects With	Prevent Alterations	EMB-06	Mechanisms exist to protect embedded devices by preventing the unauthorized installation and execution of software.	8	
IOT-06	N/A	For IoT devices that operate with a real-time operating system (RTOS), ensure that the RTOS provides a minimum set of security features including application sandboxing, secure boot, access controls, trusted execution environment, kernel separation, and a (minimized) microkernel.	Functional	Subset Of	Real-Time Operating System (RTOS) Security	EMB-18	Mechanisms exist to ensure embedded technologies utilize a securely configured Real-Time Operating System (RTOS).	10	
IOT-07	N/A	Acquire IoT devices that integrate MCUs with hardware-based separation architectures to meet high-assurance requirements. Configure security-sensitive applications to run within the hardware's trusted zone. Configure device attestation of software before entering into the trusted mode.	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
IOT-07	N/A	Acquire IoT devices that integrate MCUs with hardware-based separation architectures to meet high-assurance requirements. Configure security-sensitive applications to run within the hardware's trusted zone. Configure device attestation of software before entering into the trusted mode.	Functional	Intersects With	Operating Environment Certification	EMB-14	Mechanisms exist to determine if embedded technologies are certified for secure use in the proposed operating environment.	8	
IOT-07	N/A	Acquire IoT devices that integrate MCUs with hardware-based separation architectures to meet high-assurance requirements. Configure security-sensitive applications to run within the hardware's trusted zone. Configure device attestation of software before entering into the trusted mode.	Functional	Intersects With	Real-Time Operating System (RTOS) Security	EMB-18	Mechanisms exist to ensure embedded technologies utilize a securely configured Real-Time Operating System (RTOS).	5	
IOT-08	N/A	When deploying IoT devices in regulated industries (e.g., safety-critical environments), ensure that acquired devices use operating systems certified for use in their respective environments (airborne, industrial control, medical devices, transportation, etc.).	Functional	Intersects With	Embedded Technology Reviews	EMB-10	Mechanisms exist to perform evaluations of deployed embedded technologies as needed, or at least on an annual basis, to ensure that necessary updates to mitigate the risks associated with legacy embedded technologies are identified and implemented.	8	
IOT-08	N/A	When deploying IoT devices in regulated industries (e.g., safety-critical environments), ensure that acquired devices use operating systems certified for use in their respective environments (airborne, industrial control, medical devices, transportation, etc.).	Functional	Intersects With	Operating Environment Certification	EMB-14	Mechanisms exist to determine if embedded technologies are certified for secure use in the proposed operating environment.	8	
IOT-09	N/A	Deploy IoT devices that integrate hardware security mechanisms and use hardware roots of trust to store cryptographic material and secure operation of cryptographic functions, including secure boot and firmware signature validation.	Functional	Intersects With	Roots of Trust Protection	AST-18	Mechanisms exist to provision and protect the confidentiality, integrity and authenticity of product supplier keys and data that can be used as a "roots of trust" basis for integrity verification.	5	
IOT-09	N/A	Deploy IoT devices that integrate hardware security mechanisms and use hardware roots of trust to store cryptographic material and secure operation of cryptographic functions, including secure boot and firmware signature validation.	Functional	Intersects With	Real-Time Operating System (RTOS) Security	EMB-18	Mechanisms exist to ensure embedded technologies utilize a securely configured Real-Time Operating System (RTOS).	5	
IOT-10	N/A	Only deploy IoT gateways that are validated as Federal Information Processing Standard Publication (FIPS) 140-2 or above.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
IOT-10	N/A	Only deploy IoT gateways that are validated as Federal Information Processing Standard Publication (FIPS) 140-2 or above.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
IOT-10	N/A	Only deploy IoT gateways that are validated as Federal Information Processing Standard Publication (FIPS) 140-2 or above.	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
LGL-01	N/A	Perform a legal compliance assessment for an IoT system. Determine applicable jurisdictions, specific legislation, regulations, or any additional legalities. Include general security and privacy legislation, device-specific, age-specific (children's rights), industry-specific, and others. Know the definition of personal data, personally identifiable information, and related terms for all relevant jurisdictions to comply with requirements. Interpret legal rules in respect of the IoT system. Assess how to comply. Consider any standards that are applicable that may assist in justifying measures taken. Consider roles in the IoT system and which rules apply, as this could impact legal obligations. Take legal advice. Also, recognize potential upcoming legislation. Contemplate what aspects of the IoT system, logging, and reporting may be used in legal proceedings.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	8	
LGL-01	N/A	Perform a legal compliance assessment for an IoT system. Determine applicable jurisdictions, specific legislation, regulations, or any additional legalities. Include general security and privacy legislation, device-specific, age-specific (children's rights), industry-specific, and others. Know the definition of personal data, personally identifiable information, and related terms for all relevant jurisdictions to comply with requirements. Interpret legal rules in respect of the IoT system. Assess how to comply. Consider any standards that are applicable that may assist in justifying measures taken. Consider roles in the IoT system and which rules apply, as this could impact legal obligations. Take legal advice. Also, recognize potential upcoming legislation. Contemplate what aspects of the IoT system, logging, and reporting may be used in legal proceedings.	Functional	Intersects With	Operating Environment Certification	EMB-14	Mechanisms exist to determine if embedded technologies are certified for secure use in the proposed operating environment.	8	
LGL-01	N/A	Perform a legal compliance assessment for an IoT system. Determine applicable jurisdictions, specific legislation, regulations, or any additional legalities. Include general security and privacy legislation, device-specific, age-specific (children's rights), industry-specific, and others. Know the definition of personal data, personally identifiable information, and related terms for all relevant jurisdictions to comply with requirements. Interpret legal rules in respect of the IoT system. Assess how to comply. Consider any standards that are applicable that may assist in justifying measures taken. Consider roles in the IoT system and which rules apply, as this could impact legal obligations. Take legal advice. Also, recognize potential upcoming legislation. Contemplate what aspects of the IoT system, logging, and reporting may be used in legal proceedings.	Functional	Intersects With	Safety Assessment	EMB-15	Mechanisms exist to evaluate the safety aspects of embedded technologies via a fault tree analysis, or similar method, to determine possible consequences of misuse, misconfiguration and/or failure.	8	
LGL-01	N/A	Perform a legal compliance assessment for an IoT system. Determine applicable jurisdictions, specific legislation, regulations, or any additional legalities. Include general security and privacy legislation, device-specific, age-specific (children's rights), industry-specific, and others. Know the definition of personal data, personally identifiable information, and related terms for all relevant jurisdictions to comply with requirements. Interpret legal rules in respect of the IoT system. Assess how to comply. Consider any standards that are applicable that may assist in justifying measures taken. Consider roles in the IoT system and which rules apply, as this could impact legal obligations. Take legal advice. Also, recognize potential upcoming legislation. Contemplate what aspects of the IoT system, logging, and reporting may be used in legal proceedings.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	8	
LGL-01	N/A	Perform a legal compliance assessment for an IoT system. Determine applicable jurisdictions, specific legislation, regulations, or any additional legalities. Include general security and privacy legislation, device-specific, age-specific (children's rights), industry-specific, and others. Know the definition of personal data, personally identifiable information, and related terms for all relevant jurisdictions to comply with requirements. Interpret legal rules in respect of the IoT system. Assess how to comply. Consider any standards that are applicable that may assist in justifying measures taken. Consider roles in the IoT system and which rules apply, as this could impact legal obligations. Take legal advice. Also, recognize potential upcoming legislation. Contemplate what aspects of the IoT system, logging, and reporting may be used in legal proceedings.	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	8	
LGL-02	N/A	Create an implementation plan to comply with legal requirements for an IoT system. Include specific technical and organizational implementation of interpreted legal rules based on the IoT system. Build in measures to comply with the legal rights of consumers and/or users of the IoT system. Consider reasonable security and privacy measures where required by law. Build in mechanisms to securely collect personal or confidential data, provide data, and correct errors in data where required by law. Consider data minimization and the principle of least privilege. Consider how to block data from unauthorized individuals or organizations. Assess whether any appointments of personnel are required under the law. Conduct due diligence when approving third parties related to the IoT system.	Functional	Intersects With	Security, Compliance & Resilience in Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	
LGL-02	N/A	Create an implementation plan to comply with legal requirements for an IoT system. Include specific technical and organizational implementation of interpreted legal rules based on the IoT system. Build in measures to comply with the legal rights of consumers and/or users of the IoT system. Consider reasonable security and privacy measures where required by law. Build in mechanisms to securely collect personal or confidential data, provide data, and correct errors in data where required by law. Consider data minimization and the principle of least privilege. Consider how to block data from unauthorized individuals or organizations. Assess whether any appointments of personnel are required under the law. Conduct due diligence when approving third parties related to the IoT system.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
LGL-02	N/A	Create an implementation plan to comply with legal requirements for an IoT system. Include specific technical and organizational implementation of interpreted legal rules based on the IoT system. Build in measures to comply with the legal rights of consumers and/or users of the IoT system. Consider reasonable security and privacy measures where required by law. Build in mechanisms to securely collect personal or confidential data, provide data, and correct errors in data where required by law. Consider data minimization and the principle of least privilege. Consider how to block data from unauthorized individuals or organizations. Assess whether any appointments of personnel are required under the law. Conduct due diligence when approving third parties related to the IoT system.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
LGL-02	N/A	Create an implementation plan to comply with legal requirements for an IoT system. Include specific technical and organizational implementation of interpreted legal rules based on the IoT system. Build in measures to comply with the legal rights of consumers and/or users of the IoT system. Consider reasonable security and privacy measures where required by law. Build in mechanisms to securely collect personal or confidential data, provide data, and correct errors in data where required by law. Consider data minimization and the principle of least privilege. Consider how to block data from unauthorized individuals or organizations. Assess whether any appointments of personnel are required under the law. Conduct due diligence when approving third parties related to the IoT system.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
LGL-03	N/A	Document major security and privacy measures with a justification of how these comply with the law as instructed by counsel.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	8	
LGL-03	N/A	Document major security and privacy measures with a justification of how these comply with the law as instructed by counsel.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	8	
LGL-03	N/A	Document major security and privacy measures with a justification of how these comply with the law as instructed by counsel.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	8	
LGL-03	N/A	Document major security and privacy measures with a justification of how these comply with the law as instructed by counsel.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	8	
LGL-03	N/A	Document major security and privacy measures with a justification of how these comply with the law as instructed by counsel.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	8	
LGL-03	N/A	Document major security and privacy measures with a justification of how these comply with the law as instructed by counsel.	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	8	
LGL-04	N/A	Create a set of terms and conditions and a privacy policy associated with an IoT system and specific devices as required by law or recommended. Consider data collected, whether it will be personal data/confidential data or identifiable to an individual, data use, whether it can be or will be sold to any parties, and whether instances of future data collection may arise. Ensure compliance with all jurisdictions. Create a separate privacy policy or a supplemental privacy policy as needed for specific jurisdictions. Have this reviewed by legal counsel. Do not overpromise privacy or engage in deceptive or unfair practices; these may be used against an organization. Obtain informed consent to terms and conditions as well as the privacy policy. Ensure these are agreed to as a contract in relevant jurisdictions.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	8	
LGL-04	N/A	Create a set of terms and conditions and a privacy policy associated with an IoT system and specific devices as required by law or recommended. Consider data collected, whether it will be personal data/confidential data or identifiable to an individual, data use, whether it can be or will be sold to any parties, and whether instances of future data collection may arise. Ensure compliance with all jurisdictions. Create a separate privacy policy or a supplemental privacy policy as needed for specific jurisdictions. Have this reviewed by legal counsel. Do not overpromise privacy or engage in deceptive or unfair practices; these may be used against an organization. Obtain informed consent to terms and conditions as well as the privacy policy. Ensure these are agreed to as a contract in relevant jurisdictions.	Functional	Intersects With	Data Privacy Program	PRM-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	8	
LGL-04	N/A	Create a set of terms and conditions and a privacy policy associated with an IoT system and specific devices as required by law or recommended. Consider data collected, whether it will be personal data/confidential data or identifiable to an individual, data use, whether it can be or will be sold to any parties, and whether instances of future data collection may arise. Ensure compliance with all jurisdictions. Create a separate privacy policy or a supplemental privacy policy as needed for specific jurisdictions. Have this reviewed by legal counsel. Do not overpromise privacy or engage in deceptive or unfair practices; these may be used against an organization. Obtain informed consent to terms and conditions as well as the privacy policy. Ensure these are agreed to as a contract in relevant jurisdictions.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	8	
LGL-04	N/A	Create a set of terms and conditions and a privacy policy associated with an IoT system and specific devices as required by law or recommended. Consider data collected, whether it will be personal data/confidential data or identifiable to an individual, data use, whether it can be or will be sold to any parties, and whether instances of future data collection may arise. Ensure compliance with all jurisdictions. Create a separate privacy policy or a supplemental privacy policy as needed for specific jurisdictions. Have this reviewed by legal counsel. Do not overpromise privacy or engage in deceptive or unfair practices; these may be used against an organization. Obtain informed consent to terms and conditions as well as the privacy policy. Ensure these are agreed to as a contract in relevant jurisdictions.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	8	
LGL-04	N/A	Create a set of terms and conditions and a privacy policy associated with an IoT system and specific devices as required by law or recommended. Consider data collected, whether it will be personal data/confidential data or identifiable to an individual, data use, whether it can be or will be sold to any parties, and whether instances of future data collection may arise. Ensure compliance with all jurisdictions. Create a separate privacy policy or a supplemental privacy policy as needed for specific jurisdictions. Have this reviewed by legal counsel. Do not overpromise privacy or engage in deceptive or unfair practices; these may be used against an organization. Obtain informed consent to terms and conditions as well as the privacy policy. Ensure these are agreed to as a contract in relevant jurisdictions.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
LGL-05	N/A	Consider all the necessary contracts. Include indemnification clauses where applicable. Consider security and privacy areas and relevant responsibilities. Obtain consent where required. Weigh jurisdictional requirements and enforceability of contracts. These considerations may include agreements with organizations in jurisdictions where the likelihood of enforcement is unlikely or very difficult. Consider enforceability of clauses in particular jurisdictions. A law in one jurisdiction may not be applicable in another; consider this carefully.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	8	
LGL-05	N/A	Consider all the necessary contracts. Include indemnification clauses where applicable. Consider security and privacy areas and relevant responsibilities. Obtain consent where required. Weigh jurisdictional requirements and enforceability of contracts. These considerations may include agreements with organizations in jurisdictions where the likelihood of enforcement is unlikely or very difficult. Consider enforceability of clauses in particular jurisdictions. A law in one jurisdiction may not be applicable in another; consider this carefully.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	8	
LGL-05	N/A	Consider all the necessary contracts. Include indemnification clauses where applicable. Consider security and privacy areas and relevant responsibilities. Obtain consent where required. Weigh jurisdictional requirements and enforceability of contracts. These considerations may include agreements with organizations in jurisdictions where the likelihood of enforcement is unlikely or very difficult. Consider enforceability of clauses in particular jurisdictions. A law in one jurisdiction may not be applicable in another; consider this carefully.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	8	
LGL-05	N/A	Consider all the necessary contracts. Include indemnification clauses where applicable. Consider security and privacy areas and relevant responsibilities. Obtain consent where required. Weigh jurisdictional requirements and enforceability of contracts. These considerations may include agreements with organizations in jurisdictions where the likelihood of enforcement is unlikely or very difficult. Consider enforceability of clauses in particular jurisdictions. A law in one jurisdiction may not be applicable in another; consider this carefully.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	8	
LGL-05	N/A	Consider all the necessary contracts. Include indemnification clauses where applicable. Consider security and privacy areas and relevant responsibilities. Obtain consent where required. Weigh jurisdictional requirements and enforceability of contracts. These considerations may include agreements with organizations in jurisdictions where the likelihood of enforcement is unlikely or very difficult. Consider enforceability of clauses in particular jurisdictions. A law in one jurisdiction may not be applicable in another; consider this carefully.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	8	
LGL-06	N/A	Create necessary disclosures, disclaimers, and waivers related to the IoT system to protect the organization. Consider third-party liability. Consider all required consumers and/or other stakeholders. Review breach notification rules and anticipate how to best react in the event of a breach.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	8	
LGL-06	N/A	Create necessary disclosures, disclaimers, and waivers related to the IoT system to protect the organization. Consider third-party liability. Consider all required consumers and/or other stakeholders. Review breach notification rules and anticipate how to best react in the event of a breach.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	8	
LGL-06	N/A	Create necessary disclosures, disclaimers, and waivers related to the IoT system to protect the organization. Consider third-party liability. Consider all required consumers and/or other stakeholders. Review breach notification rules and anticipate how to best react in the event of a breach.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
LGL-06	N/A	Create necessary disclosures, disclaimers, and waivers related to the IoT system to protect the organization. Consider third-party liability. Consider all required consumers and/or other stakeholders. Review breach notification rules and anticipate how to best react in the event of a breach.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	8	
LGL-06	N/A	Create necessary disclosures, disclaimers, and waivers related to the IoT system to protect the organization. Consider third-party liability. Consider all required consumers and/or other stakeholders. Review breach notification rules and anticipate how to best react in the event of a breach.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	8	
LGL-07	N/A	Consider all major liability areas associated with an IoT system. Consider possible legal exposure within the IoT system that might result from something the organization can control. Consider areas outside of an organization's control and whether these are addressed in liability disclaimers. Create and implement a plan to address significant areas of potential liability after understanding risks.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	8	
LGL-07	N/A	Consider all major liability areas associated with an IoT system. Consider possible legal exposure within the IoT system that might result from something the organization can control. Consider areas outside of an organization's control and whether these are addressed in liability disclaimers. Create and implement a plan to address significant areas of potential liability after understanding risks.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a critically analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	8	
LGL-07	N/A	Consider all major liability areas associated with an IoT system. Consider possible legal exposure within the IoT system that might result from something the organization can control. Consider areas outside of an organization's control and whether these are addressed in liability disclaimers. Create and implement a plan to address significant areas of potential liability after understanding risks.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	8	
LGL-07	N/A	Consider all major liability areas associated with an IoT system. Consider possible legal exposure within the IoT system that might result from something the organization can control. Consider areas outside of an organization's control and whether these are addressed in liability disclaimers. Create and implement a plan to address significant areas of potential liability after understanding risks.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	8	
LGL-07	N/A	Consider all major liability areas associated with an IoT system. Consider possible legal exposure within the IoT system that might result from something the organization can control. Consider areas outside of an organization's control and whether these are addressed in liability disclaimers. Create and implement a plan to address significant areas of potential liability after understanding risks.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	8	
LGL-08	N/A	Consider any applicable rules or restrictions on data transfer and comply with the same guidelines.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	8	
LGL-08	N/A	Consider any applicable rules or restrictions on data transfer and comply with the same guidelines.	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	8	
LGL-08	N/A	Consider any applicable rules or restrictions on data transfer and comply with the same guidelines.	Functional	Intersects With	Geographic Location of Data	DCH-19	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physical and virtual), infrastructure, systems components and/or shared with other third-parties.	8	
LGL-08	N/A	Consider any applicable rules or restrictions on data transfer and comply with the same guidelines.	Functional	Intersects With	Transfer of Sensitive and/or Regulated Data	DCH-25	Mechanisms exist to restrict and govern the transfer of sensitive and/or regulated data to third-countries or international organizations.	8	
LGL-08	N/A	Consider any applicable rules or restrictions on data transfer and comply with the same guidelines.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a critically analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	8	
LGL-08	N/A	Consider any applicable rules or restrictions on data transfer and comply with the same guidelines.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	8	
LGL-08	N/A	Consider any applicable rules or restrictions on data transfer and comply with the same guidelines.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	8	
MON-01	N/A	Implement monitoring rules to detect multiple IoT device authentications when they have identical identity credentials. Such a scenario may indicate an IoT device credential compromise or non-adherence to security best practices (associated with provisioning unique credentials to each IoT device). Investigate and remediate issues upon detection.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
MON-01	N/A	Implement monitoring rules to detect multiple IoT device authentications when they have identical identity credentials. Such a scenario may indicate an IoT device credential compromise or non-adherence to security best practices (associated with provisioning unique credentials to each IoT device). Investigate and remediate issues upon detection.	Functional	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on indicators of compromise (IOC).	8	
MON-01	N/A	Implement monitoring rules to detect multiple IoT device authentications when they have identical identity credentials. Such a scenario may indicate an IoT device credential compromise or non-adherence to security best practices (associated with provisioning unique credentials to each IoT device). Investigate and remediate issues upon detection.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	8	
MON-02	N/A	Define security-relevant events to include elevation of privilege attempts, successful/unsuccessful firmware update events, configuration changes to IoT devices and service software, account modifications, tamper events, etc.). Monitor these security events across the entire IoT system, including all devices, cloud services, mobile or network services, and storage systems.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	8	
MON-02	N/A	Define security-relevant events to include elevation of privilege attempts, successful/unsuccessful firmware update events, configuration changes to IoT devices and service software, account modifications, tamper events, etc.). Monitor these security events across the entire IoT system, including all devices, cloud services, mobile or network services, and storage systems.	Functional	Intersects With	Indicators of Compromise (IOC)	IRO-03	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	8	
MON-03	N/A	Log every failed remote access attempt (secure socket shell (SSH), web, etc.). Send an alert to a security administrator for resolution when detecting five sequential invalid attempts over a 30-minute period.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
MON-03	N/A	Log every failed remote access attempt (secure socket shell (SSH), web, etc.). Send an alert to a security administrator for resolution when detecting five sequential invalid attempts over a 30-minute period.	Functional	Intersects With	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	8	
MON-03	N/A	Log every failed remote access attempt (secure socket shell (SSH), web, etc.). Send an alert to a security administrator for resolution when detecting five sequential invalid attempts over a 30-minute period.	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	8	
MON-03	N/A	Log every failed remote access attempt (secure socket shell (SSH), web, etc.). Send an alert to a security administrator for resolution when detecting five sequential invalid attempts over a 30-minute period.	Functional	Intersects With	Automated Alerts	MON-01.12	Mechanisms exist to automatically alert incident response personnel to inappropriate or anomalous activities that have potential security incident implications.	5	
MON-03	N/A	Log every failed remote access attempt (secure socket shell (SSH), web, etc.). Send an alert to a security administrator for resolution when detecting five sequential invalid attempts over a 30-minute period.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	8	
MON-04	N/A	Implement an audit user group responsible for managing (e.g., reviewing or rotating off device) audit log data. Restrict read access to security logs to this group membership. Provision audit group members with read access but do not provide write privileges to any audit logs.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	8	
MON-04	N/A	Implement an audit user group responsible for managing (e.g., reviewing or rotating off device) audit log data. Restrict read access to security logs to this group membership. Provision audit group members with read access but do not provide write privileges to any audit logs.	Functional	Subset Of	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	10	
MON-04	N/A	Implement an audit user group responsible for managing (e.g., reviewing or rotating off device) audit log data. Restrict read access to security logs to this group membership. Provision audit group members with read access but do not provide write privileges to any audit logs.	Functional	Intersects With	Access by Subset of Privileged Users	MON-08.2	Mechanisms exist to restrict access to the management of event logs to privileged users with a specific business need.	8	
MON-05	N/A	Document all logging mechanisms. Verify that only assigned audit group members can read audit logs, and no other users can write the logs. Ensure the offload of audit log data (e.g., from device to cloud or gateway) is integrity-protected (e.g., hash message authentication code (HMAC) or digital signature) and that integrity protection is maintained with the log during long-term storage. In all cases, validate the integrity of log files before review.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
MON-05	N/A	Document all logging mechanisms. Verify that only assigned audit group members can read audit logs, and no other users can write the logs. Ensure the offload of audit log data (e.g., from device to cloud or gateway) is integrity-protected (e.g., hash message authentication code (HMAC) or digital signature) and that integrity protection is maintained with the log during long-term storage. In all cases, validate the integrity of log files before review.	Functional	Intersects With	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	8	
MON-05	N/A	Document all logging mechanisms. Verify that only assigned audit group members can read audit logs, and no other users can write the logs. Ensure the offload of audit log data (e.g., from device to cloud or gateway) is integrity-protected (e.g., hash message authentication code (HMAC) or digital signature) and that integrity protection is maintained with the log during long-term storage. In all cases, validate the integrity of log files before review.	Functional	Intersects With	Event Log Backup on Separate Physical Systems / Components	MON-08.1	Mechanisms exist to back up event logs onto a physically different system or system component than the Security Incident Event Manager (SIEM) or similar automated tool.	8	
MON-05	N/A	Document all logging mechanisms. Verify that only assigned audit group members can read audit logs, and no other users can write the logs. Ensure the offload of audit log data (e.g., from device to cloud or gateway) is integrity-protected (e.g., hash message authentication code (HMAC) or digital signature) and that integrity protection is maintained with the log during long-term storage. In all cases, validate the integrity of log files before review.	Functional	Intersects With	Access by Subset of Privileged Users	MON-08.2	Mechanisms exist to restrict access to the management of event logs to privileged users with a specific business need.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
MON-05	N/A	Document all logging mechanisms. Verify that only assigned audit group members can read audit logs, and no other users can write the logs. Ensure the payload of audit log data (e.g., from device to cloud or gateway) is integrity-protected (e.g., hash message authentication code (HMAC) or digital signature) and that integrity protection is maintained with the log during long-term storage. In all cases, validate the integrity of log files before review.	Functional	Intersects With	Cryptographic Protection of Event Log Information	MON-08.3	Cryptographic mechanisms exist to protect the integrity of event logs and audit tools.	8	
MON-06	N/A	Automatically transmit security event data to the cloud for storage and analysis and records, at minimum, the initiator, receiver, timestamp, data, and event types.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	8	
MON-06	N/A	Automatically transmit security event data to the cloud for storage and analysis and records, at minimum, the initiator, receiver, timestamp, data, and event types.	Functional	Intersects With	Event Log Backup on Separate Physical Systems / Components	MON-08.1	Mechanisms exist to back up event logs onto a physically different system or system component than the Security Incident Event Manager (SIEM) or similar automated tool.	8	
MON-07	N/A	Design and implement an enterprise logging capability. Integrity protect all logs from generation to storage to enable a chain of custody.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
MON-07	N/A	Design and implement an enterprise logging capability. Integrity protect all logs from generation to storage to enable a chain of custody.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	8	
MON-07	N/A	Design and implement an enterprise logging capability. Integrity protect all logs from generation to storage to enable a chain of custody.	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	8	
MON-07	N/A	Design and implement an enterprise logging capability. Integrity protect all logs from generation to storage to enable a chain of custody.	Functional	Intersects With	System-Wide / Time-Correlated Audit Trail	MON-02.7	Automated mechanisms exist to compile audit records into an organization-wide audit trail that is time-correlated.	8	
MON-08	N/A	Establish an enterprise IoT wireless detection capability. Actively search the network for rogue wireless devices. Actively search for network communications to well-known botnet customer to customer (C2C) addresses/ports. Actively search for unauthorized communications to vendor IP addresses. Immediately disable any identified devices/communications and investigate infraction causes. Take action to educate users when unintended violations occur.	Functional	Intersects With	Wireless Network Monitoring	MON-01.5	Mechanisms exist to monitor wireless network segments for: (1) Rogue wireless devices; and (2) Anomalous and/or hostile activities.	8	
MON-08	N/A	Establish an enterprise IoT wireless detection capability. Actively search the network for rogue wireless devices. Actively search for network communications to well-known botnet customer to customer (C2C) addresses/ports. Actively search for unauthorized communications to vendor IP addresses. Immediately disable any identified devices/communications and investigate infraction causes. Take action to educate users when unintended violations occur.	Functional	Intersects With	Wireless Intrusion Detection / Prevention Systems (WIDS / WIPS) Deployment	NET-08.2	Mechanisms exist to utilize Wireless Intrusion Detection / Protection Systems (WIDS / WIPS) on wireless network segments.	8	
MON-09	N/A	Actively search for indicators of compromise, such as new botnet activity, immediately remove infected IoT devices upon detection.	Functional	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on indicators of compromise (IOC).	8	
MON-09	N/A	Actively search for indicators of compromise, such as new botnet activity, immediately remove infected IoT devices upon detection.	Functional	Intersects With	Indicators of Compromise (IOC)	IRO-03	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	8	
MON-10	N/A	Monitor wired/wireless network communication to identify rogue devices and abnormal behavior.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	8	
MON-11	N/A	Identify threat intelligence feeds applicable to specific industries. Then, maintain an understanding of attacker types that typically target particular systems and their motivations.	Functional	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on indicators of compromise (IOC).	8	
MON-11	N/A	Identify threat intelligence feeds applicable to specific industries. Then, maintain an understanding of attacker types that typically target particular systems and their motivations.	Functional	Intersects With	Indicators of Compromise (IOC)	IRO-03	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	8	
MON-11	N/A	Identify threat intelligence feeds applicable to specific industries. Then, maintain an understanding of attacker types that typically target particular systems and their motivations.	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	8	
OPA-01	N/A	Create maintenance plans to inspect and upkeep IoT hardware routinely. Keep parts on hand in inventory in case an IoT device requires repair or replacement. Take immediate action when a maintenance issue is identified by repairing or replacing the IoT device.	Functional	Intersects With	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	5	
OPA-01	N/A	Create maintenance plans to inspect and upkeep IoT hardware routinely. Keep parts on hand in inventory in case an IoT device requires repair or replacement. Take immediate action when a maintenance issue is identified by repairing or replacing the IoT device.	Functional	Intersects With	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Services (TAAS).	5	
OPA-01	N/A	Create maintenance plans to inspect and upkeep IoT hardware routinely. Keep parts on hand in inventory in case an IoT device requires repair or replacement. Take immediate action when a maintenance issue is identified by repairing or replacing the IoT device.	Functional	Intersects With	Timely Maintenance	MNT-03	Mechanisms exist to obtain maintenance support and/or spare parts for Technology Assets, Applications and/or Services (TAAS) within a defined Recovery Time Objective (RTO).	5	
OPA-01	N/A	Create maintenance plans to inspect and upkeep IoT hardware routinely. Keep parts on hand in inventory in case an IoT device requires repair or replacement. Take immediate action when a maintenance issue is identified by repairing or replacing the IoT device.	Functional	Intersects With	Preventative Maintenance	MNT-03.1	Mechanisms exist to perform preventive maintenance on critical Technology Assets, Applications and/or Services (TAAS).	5	
OPA-02	N/A	Use predictive maintenance analysis to calculate expected performance issues or breakdowns in IoT systems. Act on that data as needed.	Functional	Intersects With	Automated Support For Predictive Maintenance	MNT-03.3	Automated mechanisms exist to transfer predictive maintenance data to a computerized maintenance management system.	8	
OPA-03	N/A	Architect cloud services to support regional failover of nodes and gateways. Test annually to ensure that failover is automatic if a single region is brought offline.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
OPA-03	N/A	Architect cloud services to support regional failover of nodes and gateways. Test annually to ensure that failover is automatic if a single region is brought offline.	Functional	Intersects With	Failover Capability	BCD-12.2	Mechanisms exist to implement real-time or near-real-time failover capability to maintain availability of critical Technology Assets, Applications, Services and/or Data (TAASD).	8	
OPA-03	N/A	Architect cloud services to support regional failover of nodes and gateways. Test annually to ensure that failover is automatic if a single region is brought offline.	Functional	Intersects With	Regional Delivery	CAP-06	Mechanisms exist to support operations that are geographically dispersed via regional delivery of technological Technology Assets, Applications and/or Services (TAAS).	5	
OPA-04	N/A	Setup monitoring procedures to identify and alert on abnormally heavy traffic transmitted from IoT devices.	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS / IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	8	
OPA-04	N/A	Setup monitoring procedures to identify and alert on abnormally heavy traffic transmitted from IoT devices.	Functional	Intersects With	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near-real-time analysis and incident escalation.	8	
OPA-04	N/A	Setup monitoring procedures to identify and alert on abnormally heavy traffic transmitted from IoT devices.	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	8	
OPA-04	N/A	Setup monitoring procedures to identify and alert on abnormally heavy traffic transmitted from IoT devices.	Functional	Intersects With	Alert Threshold Tuning	MON-01.13	Mechanisms exist to "tune" event monitoring technologies through analyzing communications traffic/event patterns and developing profiles representing common traffic patterns and/or events.	8	
OPA-05	N/A	Work with CSPs to define service-level agreements (SLAs) for uptime percentages and response timing (for incidents/patches) and hold CSPs accountable for SLA breaches.	Functional	Intersects With	Coordinate With External Service Providers	BCD-01.2	Mechanisms exist to coordinate internal contingency plans with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.	3	
OPA-05	N/A	Work with CSPs to define service-level agreements (SLAs) for uptime percentages and response timing (for incidents/patches) and hold CSPs accountable for SLA breaches.	Functional	Intersects With	Continue Essential Mission & Business Functions	BCD-02.2	Mechanisms exist to continue essential missions and business functions with little or no loss of operational continuity and sustain that continuity until full system restoration at primary processing and/or storage sites.	8	
OPA-05	N/A	Work with CSPs to define service-level agreements (SLAs) for uptime percentages and response timing (for incidents/patches) and hold CSPs accountable for SLA breaches.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
OPA-05	N/A	Work with CSPs to define service-level agreements (SLAs) for uptime percentages and response timing (for incidents/patches) and hold CSPs accountable for SLA breaches.	Functional	Intersects With	Third-Party Incident Response & Recovery Capabilities	TPM-11	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	3	
OPA-06	N/A	Architect wireless sensor network (WSN) gateways in a cluster formation to better handle heavy loads and support failover if a single gateway is brought offline. Configure IoT nodes to contact backup gateways in case a primary gateway fails. Test failover capabilities and load shedding/distribution capabilities at least annually.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
OPA-06	N/A	Architect wireless sensor network (WSN) gateways in a cluster formation to better handle heavy loads and support failover if a single gateway is brought offline. Configure IoT nodes to contact backup gateways in case a primary gateway fails. Test failover capabilities and load shedding/distribution capabilities at least annually.	Functional	Intersects With	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstruction	BCD-12	Mechanisms exist to ensure the secure recovery and reconstruction of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	5	
OPA-06	N/A	Architect wireless sensor network (WSN) gateways in a cluster formation to better handle heavy loads and support failover if a single gateway is brought offline. Configure IoT nodes to contact backup gateways in case a primary gateway fails. Test failover capabilities and load shedding/distribution capabilities at least annually.	Functional	Intersects With	Failover Capability	BCD-12.2	Mechanisms exist to implement real-time or near-real-time failover capability to maintain availability of critical Technology Assets, Applications, Services and/or Data (TAASD).	5	
OPA-06	N/A	Architect wireless sensor network (WSN) gateways in a cluster formation to better handle heavy loads and support failover if a single gateway is brought offline. Configure IoT nodes to contact backup gateways in case a primary gateway fails. Test failover capabilities and load shedding/distribution capabilities at least annually.	Functional	Intersects With	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	3	
OPA-06	N/A	Architect wireless sensor network (WSN) gateways in a cluster formation to better handle heavy loads and support failover if a single gateway is brought offline. Configure IoT nodes to contact backup gateways in case a primary gateway fails. Test failover capabilities and load shedding/distribution capabilities at least annually.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	3	
OPA-07	N/A	Architect metropolitan-scale WSN deployments using clusters of nodes deployed to geographic regions to minimize points of interconnection and reduce long-haul traffic.	Functional	Intersects With	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	3	
OPA-07	N/A	Architect metropolitan-scale WSN deployments using clusters of nodes deployed to geographic regions to minimize points of interconnection and reduce long-haul traffic.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	3	
OPA-08	N/A	Deploy network monitoring tools and monitor IoT networks for congestion. Establish prioritized traffic flows (e.g., differentiated services) or execute dynamic rerouting (e.g., WSN/software-defined networking (SDN)) upon detection of congested communications.	Functional	Intersects With	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	8	
OPA-08	N/A	Deploy network monitoring tools and monitor IoT networks for congestion. Establish prioritized traffic flows (e.g., differentiated services) or execute dynamic rerouting (e.g., WSN/software-defined networking (SDN)) upon detection of congested communications.	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5	
OPA-08	N/A	Deploy network monitoring tools and monitor IoT networks for congestion. Establish prioritized traffic flows (e.g., differentiated services) or execute dynamic rerouting (e.g., WSN/software-defined networking (SDN)) upon detection of congested communications.	Functional	Intersects With	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
OPA-08	N/A	Deploy network monitoring tools and monitor IoT networks for congestion. Establish prioritized traffic flows (e.g., differentiated services) or execute dynamic routing (e.g., WSN/software-defined networking (SDN)) upon detection of congested communications.	Functional	Intersects With	Denial of Service (DoS) Protection	NET-02.1	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	5	
OPA-09	N/A	Cache messaging at gateways for at least one day (or more depending on your environment) to ensure the availability of messaging should IoT nodes be offline.	Functional	Intersects With	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5	
OPA-09	N/A	Cache messaging at gateways for at least one day (or more depending on your environment) to ensure the availability of messaging should IoT nodes be offline.	Functional	Intersects With	Denial of Service (DoS) Protection	NET-02.1	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	5	
PHY-01	N/A	Establish physical security processes that restrict physical access to IoT edge devices and alert on physical access attempts.	Functional	Intersects With	Kiosks & Point of Interaction (PoI) Devices	AST-07	Mechanisms exist to appropriately protect devices that capture sensitive/regulate data via direct physical interaction from tampering and substitution.	8	
PHY-01	N/A	Establish physical security processes that restrict physical access to IoT edge devices and alert on physical access attempts.	Functional	Intersects With	Physical Tampering Detection	AST-08	Mechanisms exist to periodically inspect systems and system components for indicators of compromise (IOC).	5	
PHY-01	N/A	Establish physical security processes that restrict physical access to IoT edge devices and alert on physical access attempts.	Functional	Intersects With	Interface Security	EMB-04	Mechanisms exist to protect embedded devices against unauthorized use of the physical factory diagnostic and test interfaces.	8	
PHY-01	N/A	Establish physical security processes that restrict physical access to IoT edge devices and alert on physical access attempts.	Functional	Intersects With	Embedded Technology Configuration Monitoring	EMB-05	Mechanisms exist to generate log entries on embedded devices when configuration changes or attempts to access interfaces are detected.	8	
PHY-01	N/A	Establish physical security processes that restrict physical access to IoT edge devices and alert on physical access attempts.	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5	
PHY-01	N/A	Establish physical security processes that restrict physical access to IoT edge devices and alert on physical access attempts.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
PHY-01	N/A	Establish physical security processes that restrict physical access to IoT edge devices and alert on physical access attempts.	Functional	Intersects With	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	5	
PHY-01	N/A	Establish physical security processes that restrict physical access to IoT edge devices and alert on physical access attempts.	Functional	Intersects With	Intrusion Alarms / Surveillance Equipment	PES-05.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.	5	
PHY-01	N/A	Establish physical security processes that restrict physical access to IoT edge devices and alert on physical access attempts.	Functional	Intersects With	Monitoring Physical Access To Critical Systems	PES-05.2	Facility security mechanisms exist to monitor physical access to critical systems or sensitive/regulate data, in addition to the physical access monitoring of the facility.	5	
PHY-01	N/A	Establish physical security processes that restrict physical access to IoT edge devices and alert on physical access attempts.	Functional	Intersects With	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5	
POL-01	N/A	Work with suppliers and establish SLAs that cover minimum vulnerability disclosure timelines, patch update timelines, and incident management support, including support during forensic investigations.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
POL-01	N/A	Work with suppliers and establish SLAs that cover minimum vulnerability disclosure timelines, patch update timelines, and incident management support, including support during forensic investigations.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8	
POL-01	N/A	Work with suppliers and establish SLAs that cover minimum vulnerability disclosure timelines, patch update timelines, and incident management support, including support during forensic investigations.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	8	
POL-01	N/A	Work with suppliers and establish SLAs that cover minimum vulnerability disclosure timelines, patch update timelines, and incident management support, including support during forensic investigations.	Functional	Intersects With	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected Technology Assets, Applications and/or Services (TAAS) that the organization utilizes.	8	
POL-01	N/A	Work with suppliers and establish SLAs that cover minimum vulnerability disclosure timelines, patch update timelines, and incident management support, including support during forensic investigations.	Functional	Intersects With	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	8	
POL-01	N/A	Work with suppliers and establish SLAs that cover minimum vulnerability disclosure timelines, patch update timelines, and incident management support, including support during forensic investigations.	Functional	Intersects With	Third-Party Incident Response & Recovery Capabilities	TPM-11	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	8	
POL-02	N/A	Establish policies and procedures for vendor access and management of IoT devices. These policies include data that can be transmitted out of the organization (e.g., telemetry or machine data) and authorized roles and minimum access security requirements for managing the devices within the organizations' networks. Enforce these controls and monitor for abuse.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
POL-02	N/A	Establish policies and procedures for vendor access and management of IoT devices. These policies include data that can be transmitted out of the organization (e.g., telemetry or machine data) and authorized roles and minimum access security requirements for managing the devices within the organizations' networks. Enforce these controls and monitor for abuse.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	
POL-02	N/A	Establish policies and procedures for vendor access and management of IoT devices. These policies include data that can be transmitted out of the organization (e.g., telemetry or machine data) and authorized roles and minimum access security requirements for managing the devices within the organizations' networks. Enforce these controls and monitor for abuse.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8	
POL-02	N/A	Establish policies and procedures for vendor access and management of IoT devices. These policies include data that can be transmitted out of the organization (e.g., telemetry or machine data) and authorized roles and minimum access security requirements for managing the devices within the organizations' networks. Enforce these controls and monitor for abuse.	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	8	
POL-02	N/A	Establish policies and procedures for vendor access and management of IoT devices. These policies include data that can be transmitted out of the organization (e.g., telemetry or machine data) and authorized roles and minimum access security requirements for managing the devices within the organizations' networks. Enforce these controls and monitor for abuse.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	8	
POL-02	N/A	Establish policies and procedures for vendor access and management of IoT devices. These policies include data that can be transmitted out of the organization (e.g., telemetry or machine data) and authorized roles and minimum access security requirements for managing the devices within the organizations' networks. Enforce these controls and monitor for abuse.	Functional	Intersects With	Third-Party Personnel Security	TPM-06	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	5	
POL-02	N/A	Establish policies and procedures for vendor access and management of IoT devices. These policies include data that can be transmitted out of the organization (e.g., telemetry or machine data) and authorized roles and minimum access security requirements for managing the devices within the organizations' networks. Enforce these controls and monitor for abuse.	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	8	
POL-03	N/A	Document an enterprise-wide IoT cybersecurity policy. Require all IoT implementations to comply with this policy or apply for an exception. Policies should include restrictions on the implementation of un-approved/document IoT devices/cloud services. Policies should also feature minimum security controls to apply to all IoT implementations, including cryptography, monitoring, auditing, authentication, access controls, and physical security controls. All activities must adhere to an approved IoT implementation. Monitor quarterly to identify out-of-compliance implementations.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
POL-03	N/A	Document an enterprise-wide IoT cybersecurity policy. Require all IoT implementations to comply with this policy or apply for an exception. Policies should include restrictions on the implementation of un-approved/document IoT devices/cloud services. Policies should also feature minimum security controls to apply to all IoT implementations, including cryptography, monitoring, auditing, authentication, access controls, and physical security controls. All activities must adhere to an approved IoT implementation. Monitor quarterly to identify out-of-compliance implementations.	Functional	Intersects With	Embedded Technology Security Program	EMB-01	Mechanisms exist to facilitate the implementation of embedded technology controls.	8	
POL-04	N/A	For each IoT system, define end-of-life procedures for system hardware. For any hardware storing sensitive information, dispose of that hardware securely and maintain an audit log of the disposal process, including any individual who participates in that process. Secure disposal processes can include, as applicable: data sanitization, degaussing, etc.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	8	
POL-04	N/A	For each IoT system, define end-of-life procedures for system hardware. For any hardware storing sensitive information, dispose of that hardware securely and maintain an audit log of the disposal process, including any individual who participates in that process. Secure disposal processes can include, as applicable: data sanitization, degaussing, etc.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	8	
POL-04	N/A	For each IoT system, define end-of-life procedures for system hardware. For any hardware storing sensitive information, dispose of that hardware securely and maintain an audit log of the disposal process, including any individual who participates in that process. Secure disposal processes can include, as applicable: data sanitization, degaussing, etc.	Functional	Intersects With	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.	8	
POL-04	N/A	For each IoT system, define end-of-life procedures for system hardware. For any hardware storing sensitive information, dispose of that hardware securely and maintain an audit log of the disposal process, including any individual who participates in that process. Secure disposal processes can include, as applicable: data sanitization, degaussing, etc.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
POL-04	N/A	For each IoT system, define end-of-life procedures for system hardware. For any hardware storing sensitive information, dispose of that hardware securely and maintain an audit log of the disposal process, including any individual who participates in that process. Secure disposal processes can include, as applicable: data sanitization, degaussing, etc.	Functional	Intersects With	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	8	
RSM-01	N/A	Adopt and define a standardized, industry-recognized risk management methodology that considers context, risk assessment (risk identification, analysis, evaluation), treatment, monitoring, and feedback. Effective risk management supports information technology, baseline requirements, and the organization's overall business strategy, goals, and objectives.	Functional	Intersects With	Material Risks	GOV-16.1	Mechanisms exist to define criteria necessary to designate a risk as a material risk.	3	
RSM-01	N/A	Adopt and define a standardized, industry-recognized risk management methodology that considers context, risk assessment (risk identification, analysis, evaluation), treatment, monitoring, and feedback. Effective risk management supports information technology, baseline requirements, and the organization's overall business strategy, goals, and objectives.	Functional	Intersects With	Material Threats	GOV-16.2	Mechanisms exist to define criteria necessary to designate a threat as a material threat.	3	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
RSM-01	N/A	Adopt and define a standardized, industry-recognized risk management methodology that considers context, risk assessment (risk identification, analysis, evaluation), treatment, monitoring, and feedback. Effective risk management supports information technology, baseline requirements, and the organization's overall business strategy, goals, and objectives.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
RSM-01	N/A	Adopt and define a standardized, industry-recognized risk management methodology that considers context, risk assessment (risk identification, analysis, evaluation), treatment, monitoring, and feedback. Effective risk management supports information technology, baseline requirements, and the organization's overall business strategy, goals, and objectives.	Functional	Intersects With	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	8	
RSM-01	N/A	Adopt and define a standardized, industry-recognized risk management methodology that considers context, risk assessment (risk identification, analysis, evaluation), treatment, monitoring, and feedback. Effective risk management supports information technology, baseline requirements, and the organization's overall business strategy, goals, and objectives.	Functional	Intersects With	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, regulations and contractual obligations that: (1) Document the security categorization results (including supporting rationales) in the security plan for systems; and (2) Ensure the security categorization decision is reviewed and approved by the asset owner.	8	
RSM-01	N/A	Adopt and define a standardized, industry-recognized risk management methodology that considers context, risk assessment (risk identification, analysis, evaluation), treatment, monitoring, and feedback. Effective risk management supports information technology, baseline requirements, and the organization's overall business strategy, goals, and objectives.	Functional	Intersects With	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for Technology Assets, Applications and/or Services (TAAS) to prevent potential disruptions.	8	
RSM-01	N/A	Adopt and define a standardized, industry-recognized risk management methodology that considers context, risk assessment (risk identification, analysis, evaluation), treatment, monitoring, and feedback. Effective risk management supports information technology, baseline requirements, and the organization's overall business strategy, goals, and objectives.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	8	
RSM-01	N/A	Adopt and define a standardized, industry-recognized risk management methodology that considers context, risk assessment (risk identification, analysis, evaluation), treatment, monitoring, and feedback. Effective risk management supports information technology, baseline requirements, and the organization's overall business strategy, goals, and objectives.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8	
RSM-01	N/A	Adopt and define a standardized, industry-recognized risk management methodology that considers context, risk assessment (risk identification, analysis, evaluation), treatment, monitoring, and feedback. Effective risk management supports information technology, baseline requirements, and the organization's overall business strategy, goals, and objectives.	Functional	Intersects With	Risk Ranking	RSK-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities that is based on industry-recognized practices.	8	
RSM-01	N/A	Adopt and define a standardized, industry-recognized risk management methodology that considers context, risk assessment (risk identification, analysis, evaluation), treatment, monitoring, and feedback. Effective risk management supports information technology, baseline requirements, and the organization's overall business strategy, goals, and objectives.	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	8	
RSM-01	N/A	Adopt and define a standardized, industry-recognized risk management methodology that considers context, risk assessment (risk identification, analysis, evaluation), treatment, monitoring, and feedback. Effective risk management supports information technology, baseline requirements, and the organization's overall business strategy, goals, and objectives.	Functional	Intersects With	Risk Response	RSK-06.1	Mechanisms exist to ensure proper risk response actions were performed to remediate findings from security, compliance and/or resilience-related: (1) Assessments; (2) Audits; and/or (3) Incidents.	8	
RSM-01	N/A	Adopt and define a standardized, industry-recognized risk management methodology that considers context, risk assessment (risk identification, analysis, evaluation), treatment, monitoring, and feedback. Effective risk management supports information technology, baseline requirements, and the organization's overall business strategy, goals, and objectives.	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	5	
RSM-02	N/A	Implement a risk management approach to establish context, perform risk assessments (risk identification, analysis, evaluation), determine treatment, establish monitoring, create feedback procedures and processes, and formulate baseline requirements.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
RSM-02	N/A	Implement a risk management approach to establish context, perform risk assessments (risk identification, analysis, evaluation), determine treatment, establish monitoring, create feedback procedures and processes, and formulate baseline requirements.	Functional	Intersects With	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	8	
RSM-02	N/A	Implement a risk management approach to establish context, perform risk assessments (risk identification, analysis, evaluation), determine treatment, establish monitoring, create feedback procedures and processes, and formulate baseline requirements.	Functional	Intersects With	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, regulations and contractual obligations that: (1) Document the security categorization results (including supporting rationales) in the security plan for systems; and (2) Ensure the security categorization decision is reviewed and approved by the asset owner.	8	
RSM-02	N/A	Implement a risk management approach to establish context, perform risk assessments (risk identification, analysis, evaluation), determine treatment, establish monitoring, create feedback procedures and processes, and formulate baseline requirements.	Functional	Intersects With	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for Technology Assets, Applications and/or Services (TAAS) to prevent potential disruptions.	8	
RSM-02	N/A	Implement a risk management approach to establish context, perform risk assessments (risk identification, analysis, evaluation), determine treatment, establish monitoring, create feedback procedures and processes, and formulate baseline requirements.	Functional	Intersects With	Risk Ranking	RSK-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities that is based on industry-recognized practices.	8	
RSM-02	N/A	Implement a risk management approach to establish context, perform risk assessments (risk identification, analysis, evaluation), determine treatment, establish monitoring, create feedback procedures and processes, and formulate baseline requirements.	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	8	
RSM-02	N/A	Implement a risk management approach to establish context, perform risk assessments (risk identification, analysis, evaluation), determine treatment, establish monitoring, create feedback procedures and processes, and formulate baseline requirements.	Functional	Intersects With	Risk Response	RSK-06.1	Mechanisms exist to ensure proper risk response actions were performed to remediate findings from security, compliance and/or resilience-related: (1) Assessments; (2) Audits; and/or (3) Incidents.	8	
RSM-03	N/A	Evaluate the liability potential of an IoT system when that system physically interacts with the public or workers. Define safety restrictions and post warning notices to limit liability.	Functional	Intersects With	Operating Environment Certification	EMB-14	Mechanisms exist to determine if embedded technologies are certified for secure use in the proposed operating environment.	8	
RSM-03	N/A	Evaluate the liability potential of an IoT system when that system physically interacts with the public or workers. Define safety restrictions and post warning notices to limit liability.	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	8	
RSM-03	N/A	Evaluate the liability potential of an IoT system when that system physically interacts with the public or workers. Define safety restrictions and post warning notices to limit liability.	Functional	Intersects With	Limit Potential Harm	TPM-03.2	Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.	8	
SAP-01	N/A	Design and deploy autonomous systems that segment safety-critical from non-safety-critical functions.	Functional	Intersects With	Network Segmentation (microsegmentation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	8	
SAP-01	N/A	Design and deploy autonomous systems that segment safety-critical from non-safety-critical functions.	Functional	Intersects With	Security Management Subnets	NET-06.1	Mechanisms exist to implement security management subnets to isolate security tools and support components from other internal system components by implementing separate subnetworks with managed interfaces to other components of the system.	3	
SAP-01	N/A	Design and deploy autonomous systems that segment safety-critical from non-safety-critical functions.	Functional	Intersects With	Segregation From Enterprise Services	NET-06.4	Mechanisms exist to isolate sensitive/regulated data enclaves (secure zones) from corporate-provided IT resources by providing enclave-specific IT services (e.g., directory services, DNS, NTP, ITAM, anti-malware, patch management, etc.) to those isolated network segments.	3	
SAP-02	N/A	Implement environmental controls that validate the safe operation of an autonomous system and change states when safe operation is no longer assured (e.g., collaborative robotics use case).	Functional	Subset Of	Safe Operations	EMB-19	Mechanisms exist to continuously validate autonomous systems that trigger an automatic state change when safe operation is no longer assured.	10	
SAP-03	N/A	Design resilient, autonomous control systems capable of operating in sensor-degraded environments (e.g., loss of global navigation satellite system (GNSS), cameras, light detection and ranging (LIDAR), radio detection and ranging (RADAR), etc.). Use mechanisms such as mutually verifiable information, simultaneous localization and mapping (SLAM), or changing the system to a fail state.	Functional	Subset Of	Resilience To Outages	EMB-08	Mechanisms exist to configure embedded technology to be resilient to data network and power outages.	10	
SAP-05	N/A	Establish a security plan for mobile applications. Ensure mobile devices receive updates from approved/trusted repositories. Only allow the use of pre-approved mobile devices for managing IoT devices. Ensure that mobile devices store identity/key material in hardware-backed secure storage locations (e.g., Android KeyChain/KeyStore and iOS KeyChain).	Functional	Subset Of	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10	
SAP-05	N/A	Establish a security plan for mobile applications. Ensure mobile devices receive updates from approved/trusted repositories. Only allow the use of pre-approved mobile devices for managing IoT devices. Ensure that mobile devices store identity/key material in hardware-backed secure storage locations (e.g., Android KeyChain/KeyStore and iOS KeyChain).	Functional	Intersects With	Full Device & Container-Based Encryption	MDM-03	Cryptographic mechanisms exist to protect the confidentiality and integrity of information on mobile devices through full-device or container encryption.	8	
SAP-05	N/A	Establish a security plan for mobile applications. Ensure mobile devices receive updates from approved/trusted repositories. Only allow the use of pre-approved mobile devices for managing IoT devices. Ensure that mobile devices store identity/key material in hardware-backed secure storage locations (e.g., Android KeyChain/KeyStore and iOS KeyChain).	Functional	Intersects With	Personally-Owned Mobile Devices	MDM-06	Mechanisms exist to restrict the connection of personally-owned, mobile devices to organizational Technology Assets, Applications and/or Services (TAAS).	8	
SAP-05	N/A	Establish a security plan for mobile applications. Ensure mobile devices receive updates from approved/trusted repositories. Only allow the use of pre-approved mobile devices for managing IoT devices. Ensure that mobile devices store identity/key material in hardware-backed secure storage locations (e.g., Android KeyChain/KeyStore and iOS KeyChain).	Functional	Intersects With	Organization-Owned Mobile Devices	MDM-07	Mechanisms exist to prohibit the installation of non-approved applications or approved applications not obtained through the organization-approved application store.	8	
SAP-06	N/A	Implement intrusion detection/prevention capabilities within the system. Use both signature-based and behavior-based mechanisms. Behavior-based mechanisms should identify a "ground-truth" for the system and identify anomalies such as unexpected communications and behaviors.	Functional	Intersects With	File Integrity Monitoring (FIM)	MON-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical Technology Assets, Applications and/or Services (TAAS) to generate alerts for unauthorized modifications.	3	
SAP-06	N/A	Implement intrusion detection/prevention capabilities within the system. Use both signature-based and behavior-based mechanisms. Behavior-based mechanisms should identify a "ground-truth" for the system and identify anomalies such as unexpected communications and behaviors.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous activities that could indicate account compromise or other malicious activities.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
SAP-06	N/A	Implement intrusion detection/prevention capabilities within the system. Use both signature-based and behavior-based mechanisms. Behavior-based mechanisms should identify a "ground-truth" for the system and identify anomalies such as unexpected communications and behaviors.	Functional	Intersects With	Endpoint File Integrity Monitoring (FIM)	END-06	Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected files and configuration settings.	3	
SAP-06	N/A	Implement intrusion detection/prevention capabilities within the system. Use both signature-based and behavior-based mechanisms. Behavior-based mechanisms should identify a "ground-truth" for the system and identify anomalies such as unexpected communications and behaviors.	Functional	Intersects With	Host Intrusion Detection and Prevention Systems (HIDS / HIPS)	END-07	Mechanisms exist to utilize Host-based Intrusion Detection / Prevention Systems (HIDS / HIPS), or similar technologies, to monitor for and protect against anomalous host activity, including lateral movement across the network.	8	
SAP-07	N/A	Whenever possible, implement cryptographic-security processes that support authentication and integrity checking of safety-critical messages.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
SAP-07	N/A	Whenever possible, implement cryptographic-security processes that support authentication and integrity checking of safety-critical messages.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
SAP-07	N/A	Whenever possible, implement cryptographic-security processes that support authentication and integrity checking of safety-critical messages.	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	
SAP-09	N/A	Design and implement a state machine for the autonomous system. States should include fail-safe and fail-operational capabilities. Cybersecurity events should trigger state changes to one of these states. Fail operational events should require human intervention immediately.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	8	
SAP-09	N/A	Design and implement a state machine for the autonomous system. States should include fail-safe and fail-operational capabilities. Cybersecurity events should trigger state changes to one of these states. Fail operational events should require human intervention immediately.	Functional	Subset Of	Safe Operations	EMB-19	Mechanisms exist to continuously validate autonomous systems that trigger an automatic state change when safe operation is no longer assured.	10	
SAP-10	N/A	Evaluate and test operator/occupant interaction with autonomous systems to validate operator/occupant capacities to take control and/or resolve cyber anomaly issues should they occur.	Functional	Subset Of	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-01	Mechanisms exist to ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented effectively.	10	
SAP-10	N/A	Evaluate and test operator/occupant interaction with autonomous systems to validate operator/occupant capacities to take control and/or resolve cyber anomaly issues should they occur.	Functional	Intersects With	AI & Autonomous Technologies Production Monitoring	AAT-16	Mechanisms exist to monitor the functionality and behavior of the deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	8	
SAP-10	N/A	Evaluate and test operator/occupant interaction with autonomous systems to validate operator/occupant capacities to take control and/or resolve cyber anomaly issues should they occur.	Functional	Intersects With	Anomaly Detection & Human Oversight	AAT-16.11	Mechanisms exist to analyze anomalous Artificial Intelligence (AI) and Autonomous Technologies (AAT) behavior and provide escalation paths for human oversight, including: 1) Real-time review and 2) Intervention.	8	
SDV-01	N/A	Do not store API keys and other credentials in public-facing source control systems (e.g., GitLab/GitHub). Publish procedures for the secure handling of API keys. Do not hardcode API keys into firmware, mobile applications, or any client-based application. Monitor at least quarterly to verify that API keys and other credentials are not stored in public-facing source control systems.	Functional	Intersects With	Public Key Infrastructure (PKI)	CRY-08	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	8	
SDV-01	N/A	Do not store API keys and other credentials in public-facing source control systems (e.g., GitLab/GitHub). Publish procedures for the secure handling of API keys. Do not hardcode API keys into firmware, mobile applications, or any client-based application. Monitor at least quarterly to verify that API keys and other credentials are not stored in public-facing source control systems.	Functional	Subset Of	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	10	
SDV-02	N/A	Establish good supply chain practices: establish an inventory of software bill of materials (SBOM) for IoT components; subscribe to security alerts from all third-party components and frameworks; review updates to determine the timeline for applying updates; analyze change logs and release notes for security updates.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	8	
SDV-02	N/A	Establish good supply chain practices: establish an inventory of software bill of materials (SBOM) for IoT components; subscribe to security alerts from all third-party components and frameworks; review updates to determine the timeline for applying updates; analyze change logs and release notes for security updates.	Functional	Intersects With	Software Bill of Materials (SBOM)	TDA-04.2	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for Technology Assets, Applications and/or Services (TAAS) that lists software packages in use, including versions and applicable licenses.	8	
SDV-03	N/A	Adopt a software assurance maturity model (SAMM) to establish a secure development lifecycle for all developed IoT devices and components (e.g., Open Web Application Security Project (OWASP), SAMM).	Functional	Subset Of	Software Assurance Maturity Model (SAMM)	TDA-06.3	Mechanisms exist to utilize a Software Assurance Maturity Model (SAMM) to govern a secure development lifecycle for the development of Technology Assets, Applications and/or Services (TAAS).	10	
SDV-03	N/A	Adopt a software assurance maturity model (SAMM) to establish a secure development lifecycle for all developed IoT devices and components (e.g., Open Web Application Security Project (OWASP), SAMM).	Functional	Intersects With	Customized Development of Critical Components	TDA-12	Mechanisms exist to custom-develop critical system components, when Commercial Off The Shelf (COTS) solutions are unavailable.	5	
SDV-04	N/A	Use static and dynamic analysis tools to validate the authenticity, integrity, and security state of all third-party libraries used within the components of an IoT system.	Functional	Intersects With	Static Code Analysis	TDA-09.2	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ static code analysis tools to identify and remediate common flaws and document the results of the analysis.	8	
SDV-04	N/A	Use static and dynamic analysis tools to validate the authenticity, integrity, and security state of all third-party libraries used within the components of an IoT system.	Functional	Intersects With	Dynamic Code Analysis	TDA-09.3	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ dynamic code analysis tools to identify and remediate common flaws and document the results of the analysis.	8	
SDV-05	N/A	Develop applications in accordance with OWASP's Application Security Verification Standard (ASVS) and Mobile Application Security Verification Standard (MASVS) security requirements.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	8	
SDV-05	N/A	Develop applications in accordance with OWASP's Application Security Verification Standard (ASVS) and Mobile Application Security Verification Standard (MASVS) security requirements.	Functional	Intersects With	Customized Development of Critical Components	TDA-12	Mechanisms exist to custom-develop critical system components, when Commercial Off The Shelf (COTS) solutions are unavailable.	5	
SDV-06	N/A	Conduct threat modeling at the onset of any device or system development effort. Use a standardized approach to threat modeling that includes the identification of components, data flows, and high-value code. Define the threats, prioritize (e.g., rate) the threats and identify mitigations. Communicate the outputs of threat models into the system requirements backlog and track these requirements to closure across the lifecycle of the product or system.	Functional	Subset Of	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modeling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	10	
SDV-07	N/A	Perform security tests on each product and incrementally on system releases. Ensure that infrastructure-as-code (IaC) components—including container orchestration tooling—undergo static analysis testing as part of system deployment pipeline workflows.	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	8	
SDV-07	N/A	Perform security tests on each product and incrementally on system releases. Ensure that infrastructure-as-code (IaC) components—including container orchestration tooling—undergo static analysis testing as part of system deployment pipeline workflows.	Functional	Intersects With	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.	8	
SDV-07	N/A	Perform security tests on each product and incrementally on system releases. Ensure that infrastructure-as-code (IaC) components—including container orchestration tooling—undergo static analysis testing as part of system deployment pipeline workflows.	Functional	Subset Of	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and (3) Document the results.	10	
SDV-07	N/A	Perform security tests on each product and incrementally on system releases. Ensure that infrastructure-as-code (IaC) components—including container orchestration tooling—undergo static analysis testing as part of system deployment pipeline workflows.	Functional	Intersects With	Continuous Monitoring Plan	TDA-09.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a plan for the continuous monitoring of security, compliance and/or resilience control effectiveness.	8	
SDV-07	N/A	Perform security tests on each product and incrementally on system releases. Ensure that infrastructure-as-code (IaC) components—including container orchestration tooling—undergo static analysis testing as part of system deployment pipeline workflows.	Functional	Intersects With	Application Penetration Testing	TDA-09.5	Mechanisms exist to perform application-level penetration testing of custom-made Technology Assets, Applications and/or Services (TAAS).	8	
SMT-01	N/A	Securely configure all supporting networks, software, and infrastructure (e.g., web servers, cloud services, firewalls, etc.) supporting the IoT system. Refer to specific secure configuration guidance for system implementation.	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
SMT-01	N/A	Securely configure all supporting networks, software, and infrastructure (e.g., web servers, cloud services, firewalls, etc.) supporting the IoT system. Refer to specific secure configuration guidance for system implementation.	Functional	Intersects With	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	8	
SMT-01	N/A	Securely configure all supporting networks, software, and infrastructure (e.g., web servers, cloud services, firewalls, etc.) supporting the IoT system. Refer to specific secure configuration guidance for system implementation.	Functional	Intersects With	Layered Network Defenses	NET-02	Mechanisms exist to implement security functions as a layered structure that minimizes interactions between layers of the design and avoids any dependence by lower layers on the functionality or correctness of higher layers.	3	
SMT-02	N/A	Configure a software-defined perimeter (SDP) that authenticates IoT devices before network connection and restricts activities based on their pre-approved roles and privileges.	Functional	Intersects With	Zero Trust Architecture (ZTA)	NET-01.1	Mechanisms exist to treat all users and devices as potential threats and prevent access to data and resources until the users can be properly authenticated and their access authorized.	3	
SMT-03	N/A	Use a network visualization tool to monitor the operating state and health status of IoT devices, gateways, and services. Use simple heartbeat monitoring to evaluate device connectivity or simple network management protocol (SNMP)v3 traps to monitor central processing unit (CPU) utilization, memory, etc.	Functional	Intersects With	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	5	
SMT-03	N/A	Use a network visualization tool to monitor the operating state and health status of IoT devices, gateways, and services. Use simple heartbeat monitoring to evaluate device connectivity or simple network management protocol (SNMP)v3 traps to monitor central processing unit (CPU) utilization, memory, etc.	Functional	Intersects With	Performance Monitoring	CAP-04	Automated mechanisms exist to centrally-monitor and alert on the operating state and health status of critical Technology Assets, Applications and/or Services (TAAS).	5	
SMT-03	N/A	Use a network visualization tool to monitor the operating state and health status of IoT devices, gateways, and services. Use simple heartbeat monitoring to evaluate device connectivity or simple network management protocol (SNMP)v3 traps to monitor central processing unit (CPU) utilization, memory, etc.	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	
SMT-03	N/A	Use a network visualization tool to monitor the operating state and health status of IoT devices, gateways, and services. Use simple heartbeat monitoring to evaluate device connectivity or simple network management protocol (SNMP)v3 traps to monitor central processing unit (CPU) utilization, memory, etc.	Functional	Intersects With	Embedded Technology Configuration Monitoring	EMB-05	Mechanisms exist to generate log entries on embedded devices when configuration changes or attempts to access interfaces are detected.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
SMT-04	N/A	Implement authenticated discovery services. Authenticate all service discovery queries and drop requests that fail authentication.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	8	
SMT-04	N/A	Implement authenticated discovery services. Authenticate all service discovery queries and drop requests that fail authentication.	Functional	Intersects With	Automated Unauthorized Component Detection	AST-02.2	Automated mechanisms exist to detect and alert upon the detection of unauthorized hardware, software and firmware components.	8	
SMT-04	N/A	Implement authenticated discovery services. Authenticate all service discovery queries and drop requests that fail authentication.	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	8	
SMT-04	N/A	Implement authenticated discovery services. Authenticate all service discovery queries and drop requests that fail authentication.	Functional	Intersects With	Authorized Communications	EMB-13	Mechanisms exist to restrict embedded technologies to communicate only with authorized peers and service endpoints.	8	
SWS-01	N/A	Disable non-authenticated Bluetooth pairing procedures (e.g., Just Works).	Functional	Intersects With	Bluetooth & Wireless Devices	AST-14.1	Mechanisms exist to prevent the usage of Bluetooth and wireless devices (e.g., Near Field Communications (NFC)) in sensitive areas or unless used in a Radio Frequency (RF)-screened building.	8	
SWS-01	N/A	Disable non-authenticated Bluetooth pairing procedures (e.g., Just Works).	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
SWS-02	N/A	Audit the security of Bluetooth implementations using the Bluetooth security Checklist found in Section 4.4 of the NIST SP-800-121r2 document. Remediate any deficiencies.	Functional	Intersects With	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	3	
SWS-03	N/A	Install near field communication (NFC) devices in locations that do not lend themselves to installing sniffers nearby. Establish physical security protection measures (e.g., cameras/guards) to monitor access to these devices.	Functional	Intersects With	Bluetooth & Wireless Devices	AST-14.1	Mechanisms exist to prevent the usage of Bluetooth and wireless devices (e.g., Near Field Communications (NFC)) in sensitive areas or unless used in a Radio Frequency (RF)-screened building.	8	
SWS-03	N/A	Install near field communication (NFC) devices in locations that do not lend themselves to installing sniffers nearby. Establish physical security protection measures (e.g., cameras/guards) to monitor access to these devices.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	8	
SWS-04	N/A	Architect WSNs such as Zigbee, Z-Wave, LoRaWAN, and Bluetooth so that internet disconnection occurs with only authorized gateways exposing internet connectivity.	Functional	Intersects With	Limit Network Connections	NET-03.1	Mechanisms exist to limit the number of concurrent external network connections to its Technology Assets, Applications and/or Services (TAAS).	5	
SWS-04	N/A	Architect WSNs such as Zigbee, Z-Wave, LoRaWAN, and Bluetooth so that internet disconnection occurs with only authorized gateways exposing internet connectivity.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	8	
SWS-04	N/A	Architect WSNs such as Zigbee, Z-Wave, LoRaWAN, and Bluetooth so that internet disconnection occurs with only authorized gateways exposing internet connectivity.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	8	
SWS-05	N/A	Restrict device beaconing and advertisements in response to environmental threat modes.	Functional	Subset Of	Data Flow Enforcement - Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	10	
SWS-05	N/A	Restrict device beaconing and advertisements in response to environmental threat modes.	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	8	
SWS-06	N/A	Scan geographic areas for jammers attempting to suppress radio frequency (RF) communications and execute incident response plans upon detecting such an event.	Functional	Intersects With	Rogue Wireless Detection	NET-15.5	Mechanisms exist to test for the presence of Wireless Access Points (WAPs) and identify all authorized and unauthorized WAPs within the facilities).	8	
SWS-06	N/A	Scan geographic areas for jammers attempting to suppress radio frequency (RF) communications and execute incident response plans upon detecting such an event.	Functional	Intersects With	Technical Surveillance Countermeasures Security	VPM-08	Mechanisms exist to utilize a technical surveillance countermeasures survey.	8	
SWS-07	N/A	Encrypt all wireless communications within an IoT system.	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	8	
SWS-07	N/A	Encrypt all wireless communications within an IoT system.	Functional	Intersects With	Wireless Link Protection	NET-12.1	Mechanisms exist to protect external and internal wireless links from signal parameter attacks through monitoring for unauthorized wireless connections, including scanning for unauthorized wireless access points and taking appropriate action, if an unauthorized connection is discovered.	8	
SWS-08	N/A	Disable the default ZigBee trust center (TC) key and generate/use a non-default key for confidentiality protection of keys in transport.	Functional	Subset Of	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
SWS-09	N/A	Distribute ZigBee master keys out-of-band, and never pass master keys over the network.	Functional	Intersects With	Out-of-Band Channels	NET-11	Mechanisms exist to utilize out-of-band channels for the electronic transmission of information and/or the physical shipment of system components or devices to authorized individuals.	3	
SWS-10	N/A	Rotate ZigBee network keys at least annually and disable the previous keys when establishing and distributing the new network keys.	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	3	
SWS-11	N/A	Supplement Z-Wave networks with Advanced Encryption Standard (AES) 128 cryptographic keys for authentication.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
TRN-01	N/A	Establish a security training program for IoT administrators. At a minimum, include information on acceptable use policies, IoT assets used within the organization, procedures for bootstrapping trust in IoT devices, monitoring the security posture of IoT systems, approved processes for securely administering IoT devices, and incident response procedures. Require that IoT system administrators take this training annually.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
TRN-01	N/A	Establish a security training program for IoT administrators. At a minimum, include information on acceptable use policies, IoT assets used within the organization, procedures for bootstrapping trust in IoT devices, monitoring the security posture of IoT systems, approved processes for securely administering IoT devices, and incident response procedures. Require that IoT system administrators take this training annually.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	8	
TRN-02	N/A	Establish a user security training program. The training program should focus on making all personnel aware of their roles and responsibilities in maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. Training should also focus on maintaining a safe and secure working environment, including policies and procedures related to the use of employee-owned IoT devices on the corporate network (e.g., smart TVs, wearables, etc.). Training should include a discussion on the risks associated with IoT devices, privacy concerns associated with IoT devices, and procedures for interfacing with corporate IoT devices (if applicable). Require that all users of IoT systems take this training annually.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
TRN-02	N/A	Establish a user security training program. The training program should focus on making all personnel aware of their roles and responsibilities in maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. Training should also focus on maintaining a safe and secure working environment, including policies and procedures related to the use of employee-owned IoT devices on the corporate network (e.g., smart TVs, wearables, etc.). Training should include a discussion on the risks associated with IoT devices, privacy concerns associated with IoT devices, and procedures for interfacing with corporate IoT devices (if applicable). Require that all users of IoT systems take this training annually.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	8	
TRN-02	N/A	Establish a user security training program. The training program should focus on making all personnel aware of their roles and responsibilities in maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. Training should also focus on maintaining a safe and secure working environment, including policies and procedures related to the use of employee-owned IoT devices on the corporate network (e.g., smart TVs, wearables, etc.). Training should include a discussion on the risks associated with IoT devices, privacy concerns associated with IoT devices, and procedures for interfacing with corporate IoT devices (if applicable). Require that all users of IoT systems take this training annually.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	8	
TRN-02	N/A	Establish a user security training program. The training program should focus on making all personnel aware of their roles and responsibilities in maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. Training should also focus on maintaining a safe and secure working environment, including policies and procedures related to the use of employee-owned IoT devices on the corporate network (e.g., smart TVs, wearables, etc.). Training should include a discussion on the risks associated with IoT devices, privacy concerns associated with IoT devices, and procedures for interfacing with corporate IoT devices (if applicable). Require that all users of IoT systems take this training annually.	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	8	
TRN-02	N/A	Establish a user security training program. The training program should focus on making all personnel aware of their roles and responsibilities in maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. Training should also focus on maintaining a safe and secure working environment, including policies and procedures related to the use of employee-owned IoT devices on the corporate network (e.g., smart TVs, wearables, etc.). Training should include a discussion on the risks associated with IoT devices, privacy concerns associated with IoT devices, and procedures for interfacing with corporate IoT devices (if applicable). Require that all users of IoT systems take this training annually.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	8	
TRN-03	N/A	Establish responsible disclosure policies to report security research community vulnerabilities. Establish guidelines and procedures for working with independent testers that report vulnerabilities. Establish procedures to add independently-reported vulnerabilities to the system backlog for prioritization and remediation.	Functional	Subset Of	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational TAAS.	10	
VLN-01	N/A	Implement a configuration management program to track firmware, software, and hardware versions for each IoT device in inventory. Document and get firmware updates or software patches, and flag devices not current with the latest firmware or patches.	Functional	Subset Of	Vulnerability & Patch Management (VPM)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
VLN-01	N/A	Implement a configuration management program to track firmware, software, and hardware versions for each IoT device in inventory. Document and date firmware updates or software patches, and flag devices not current with the latest firmware or patches.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	8	
VLN-01	N/A	Implement a configuration management program to track firmware, software, and hardware versions for each IoT device in inventory. Document and date firmware updates or software patches, and flag devices not current with the latest firmware or patches.	Functional	Intersects With	Centralized Management of Flow Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flow remediation process.	8	
VLN-02	N/A	Monitor devices to identify those out of compliance with organizational policies and require updates or patches.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	8	
VLN-02	N/A	Monitor devices to identify those out of compliance with organizational policies and require updates or patches.	Functional	Intersects With	Centralized Management of Flow Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flow remediation process.	8	
VLN-03	N/A	Monitor for newly identified product vulnerabilities, including in product dependencies, and monitor for newly released supplier patches.	Functional	Intersects With	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	8	
VLN-03	N/A	Monitor for newly identified product vulnerabilities, including in product dependencies, and monitor for newly released supplier patches.	Functional	Intersects With	Automated Software & Firmware Updates	VPM-05.4	Automated mechanisms exist to install the latest stable versions of security-relevant software and firmware updates.	8	
VLN-04	N/A	Establish a vulnerability management program for IoT systems. Perform periodic or continuous vulnerability assessments of IoT deployments (at least annually), maintaining a risk register reflecting vulnerability information associated with deployed IoT devices/systems. Use vulnerability correlation and security orchestration tools to automate vulnerability scanning upon predefined schedules.	Functional	Intersects With	Embedded Technology Security Program	EMB-01	Mechanisms exist to facilitate the implementation of embedded technology controls.	8	
VLN-04	N/A	Establish a vulnerability management program for IoT systems. Perform periodic or continuous vulnerability assessments of IoT deployments (at least annually), maintaining a risk register reflecting vulnerability information associated with deployed IoT devices/systems. Use vulnerability correlation and security orchestration tools to automate vulnerability scanning upon predefined schedules.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMF)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	8	
VLN-04	N/A	Establish a vulnerability management program for IoT systems. Perform periodic or continuous vulnerability assessments of IoT deployments (at least annually), maintaining a risk register reflecting vulnerability information associated with deployed IoT devices/systems. Use vulnerability correlation and security orchestration tools to automate vulnerability scanning upon predefined schedules.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	8	
VLN-04	N/A	Establish a vulnerability management program for IoT systems. Perform periodic or continuous vulnerability assessments of IoT deployments (at least annually), maintaining a risk register reflecting vulnerability information associated with deployed IoT devices/systems. Use vulnerability correlation and security orchestration tools to automate vulnerability scanning upon predefined schedules.	Functional	Intersects With	Vulnerability Ranking	VPM-03	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	8	
VLN-04	N/A	Establish a vulnerability management program for IoT systems. Perform periodic or continuous vulnerability assessments of IoT deployments (at least annually), maintaining a risk register reflecting vulnerability information associated with deployed IoT devices/systems. Use vulnerability correlation and security orchestration tools to automate vulnerability scanning upon predefined schedules.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	8	
VLN-04	N/A	Establish a vulnerability management program for IoT systems. Perform periodic or continuous vulnerability assessments of IoT deployments (at least annually), maintaining a risk register reflecting vulnerability information associated with deployed IoT devices/systems. Use vulnerability correlation and security orchestration tools to automate vulnerability scanning upon predefined schedules.	Functional	Intersects With	Breadth / Depth of Coverage	VPM-06.2	Mechanisms exist to identify the breadth and depth of coverage for vulnerability scanning that define the system components scanned and types of vulnerabilities that are checked for.	8	
SET-01	N/A	Determine the assessment target IoT component(s), allocated budget, versioning, testing constraints, overall goals, and cadence with system manufacturers or owners during scoping. Consider each facet of an IoT system, such as mobile applications, hosted web applications (software as a service (SaaS)), embedded web applications, APIs, network services, wireless communication, firmware binaries, and device hardware. Prioritize critical interfaces that allow for user control and privileged access.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
SET-01	N/A	Determine the assessment target IoT component(s), allocated budget, versioning, testing constraints, overall goals, and cadence with system manufacturers or owners during scoping. Consider each facet of an IoT system, such as mobile applications, hosted web applications (software as a service (SaaS)), embedded web applications, APIs, network services, wireless communication, firmware binaries, and device hardware. Prioritize critical interfaces that allow for user control and privileged access.	Functional	Intersects With	Assessment Boundaries	IAO-01.1	Mechanisms exist to establish the scope of assessments by defining the assessment boundary, according to people, processes and technology that directly or indirectly impact the confidentiality, integrity, availability and safety of the Technology Assets, Applications, Services and/or Data (TAASD) under review.	8	
SET-01	N/A	Determine the assessment target IoT component(s), allocated budget, versioning, testing constraints, overall goals, and cadence with system manufacturers or owners during scoping. Consider each facet of an IoT system, such as mobile applications, hosted web applications (software as a service (SaaS)), embedded web applications, APIs, network services, wireless communication, firmware binaries, and device hardware. Prioritize critical interfaces that allow for user control and privileged access.	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	8	
SET-01	N/A	Determine the assessment target IoT component(s), allocated budget, versioning, testing constraints, overall goals, and cadence with system manufacturers or owners during scoping. Consider each facet of an IoT system, such as mobile applications, hosted web applications (software as a service (SaaS)), embedded web applications, APIs, network services, wireless communication, firmware binaries, and device hardware. Prioritize critical interfaces that allow for user control and privileged access.	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; and/or (11) Artificial Intelligence and Autonomous Technologies (AAT).	8	
SET-02	N/A	Perform penetration testing on IoT systems at least annually. Evaluate findings and prepare a plan to mitigate identified vulnerabilities. Perform testing on individual system components and the system as a whole using a range of tactics, techniques, and procedures. Ensure findings are prioritized for remediation. Application assessment methodologies should follow the OWASP Web Security Testing Guide against the applicable assurance levels within the OWASP Application Security Verification Standard. Firmware-related assessments should follow the OWASP Firmware Security Testing Methodology.	Functional	Intersects With	Application Penetration Testing	TDA-09.5	Mechanisms exist to perform application-level penetration testing of custom-made Technology Assets, Applications and/or Services (TAAS).	8	
SET-02	N/A	Perform penetration testing on IoT systems at least annually. Evaluate findings and prepare a plan to mitigate identified vulnerabilities. Perform testing on individual system components and the system as a whole using a range of tactics, techniques, and procedures. Ensure findings are prioritized for remediation. Application assessment methodologies should follow the OWASP Web Security Testing Guide against the applicable assurance levels within the OWASP Application Security Verification Standard. Firmware-related assessments should follow the OWASP Firmware Security Testing Methodology.	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	8	
SET-02	N/A	Perform penetration testing on IoT systems at least annually. Evaluate findings and prepare a plan to mitigate identified vulnerabilities. Perform testing on individual system components and the system as a whole using a range of tactics, techniques, and procedures. Ensure findings are prioritized for remediation. Application assessment methodologies should follow the OWASP Web Security Testing Guide against the applicable assurance levels within the OWASP Application Security Verification Standard. Firmware-related assessments should follow the OWASP Firmware Security Testing Methodology.	Functional	Intersects With	Independent Penetration Agent or Team	VPM-07.1	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	8	
SET-03	N/A	Establish red-team exercises to actively exploit IoT system vulnerabilities. Provide sufficient threat documentation to allow red team operators to identify and target weak areas. Provide red teams with adequate time to fully explore weaknesses and properly plan exploit scenarios that should be proposed before fieldwork. Assure that red-team scope includes network, application, and physical layers of the IoT system architecture. Red team testing activities should use tactics and techniques based on MITRE ATT&CK.	Functional	Intersects With	Independent Penetration Agent or Team	VPM-07.1	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	8	
SET-03	N/A	Establish red-team exercises to actively exploit IoT system vulnerabilities. Provide sufficient threat documentation to allow red team operators to identify and target weak areas. Provide red teams with adequate time to fully explore weaknesses and properly plan exploit scenarios that should be proposed before fieldwork. Assure that red-team scope includes network, application, and physical layers of the IoT system architecture. Red team testing activities should use tactics and techniques based on MITRE ATT&CK.	Functional	Intersects With	Red Team Exercises	VPM-10	Mechanisms exist to utilize "red team" exercises to simulate attempts by adversaries to compromise Technology Assets, Applications and/or Services (TAAS) in accordance with organization-defined rules of engagement.	8	
SET-04	N/A	Identify qualified third-party firms to perform IoT penetration testing fieldwork. Request relevant IoT penetration test reports to review as part of vendor intake. Ensure industry methodologies and tools are shareable to reproduce identified vulnerabilities. Consider including hardware and firmware as part of the scope for advanced security testing fieldwork to provide a complete landscape of risk.	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	8	
SET-04	N/A	Identify qualified third-party firms to perform IoT penetration testing fieldwork. Request relevant IoT penetration test reports to review as part of vendor intake. Ensure industry methodologies and tools are shareable to reproduce identified vulnerabilities. Consider including hardware and firmware as part of the scope for advanced security testing fieldwork to provide a complete landscape of risk.	Functional	Intersects With	Independent Penetration Agent or Team	VPM-07.1	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	8	
SET-05	N/A	Establish processes checks within the procurement lifecycle to validate that vendors participate in bug bounties. If possible, request manufacturer program report data for accepted bounty submissions at least annually.	Functional	Intersects With	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	5	
SET-05	N/A	Establish processes checks within the procurement lifecycle to validate that vendors participate in bug bounties. If possible, request manufacturer program report data for accepted bounty submissions at least annually.	Functional	Intersects With	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational TAAS.	5	
SET-06	N/A	Establish automated security testing into development release pipelines for all internally-developed applications and services within the IoT system against defined security requirements. Integrate static, runtime, and dynamic analysis testing into development workflows. Establish testing baselines and setup alerting for identified findings.	Functional	Subset Of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	