ID	Layer	NIST ID	Control Name	IoT Control Objective
IoT-1	1	PE-3	Physical Access Control	The manufacturer: a. Enforces physical access authorizations to the IoT device 1. Verifying individual access authorizations before granting access to the IoT device 2. Controlling ingress/egress to it b. Maintains physical access audit logs for the manufacturer c. Provides the manufacturer with control access to areas within the IoT device d. n/a, there is nothing to escort e. n/a, repetition in securing physical access to the device f. Inventories the environment of use at a manufacturer-defined frequency g. Changes combinations and keys on the IoT device when combinations are compromised
IoT-2	1	SC-8	Transmission Confidentiality and Integrity	The IoT device protects the (select one or more: confidentiality, integrity) of transmitted information.
IoT-3	2	SC-7	Boundary Protection	The IoT device: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system b. Implements subnetworks for publicly accessible system components that are (select: physically, logically) separated from internal environment of use networks c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with the manufacturer's security architecture
IoT-4	3	IA-3	Device Identification and Authentication	The IoT device uniquely identifies other devices before establishing a (select one or more: local, remote, network) connection.
IoT-5	3	SC-15	Collaborative Computing Devices	The IoT device: a. Prohibits remote activation of collaborative computing devices, except where the manufacturer explicitly allows it. b. Provides an explicit indication of use to users

				physically present at the devices
IoT-6	4	IA-2	Identification and Authentication (Organizational Users)	The IoT device uniquely identifies and authenticates manufacturer users (or processes acting on behalf of manufacturer users).
IoT-7	4	AC-2	Account Management	The manufacturer: a. Identifies and selects the system accounts to support the missions/business functions b. Assigns account managers for IoT device accounts c. Establishes conditions for group and role membership d. Specifies authorized users of the IoT device, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account e. Approves (or the owner approves) the creation of any additional IoT device accounts f. (Or the owner) creates, enables, modifies, disables, and removes IoT device accounts in accordance with manufacturer-defined procedures or conditions g. Monitors the use of IoT device system accounts h. Notifies account managers: 1.When accounts are no longer required; 2. When users are terminated or transferred 3. When individual IoT device usage or need-to-know changes i. Authorizes access to the IoT device based on: 1. A valid access authorization 2. Intended system usage 3. Other attributes as required by the manufacturer or associated missions/business functions j. Reviews accounts for compliance with account management requirements (assignment: manufacturer-defined frequency) k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group
IoT-8	5	CM-7	Least Functionality	The manufacturer: a. Configures the IoT device to provide only essential capabilities

				b. Prohibits or restricts the use of the following functions, ports, protocols and/or services (assignment: manufacturer-defined prohibited or restricted functions, ports, protocols and/or services)
IoT-9	5	SC-28	Protection of Information at Rest	The IoT device protects the (select one or more: confidentiality, integrity) of (assignment: manufacturer-defined information at rest).
IoT-10	5	PL-2	System Security Plan	The manufacturer: a. Develops a security plan for the IoT device that: 1. Is consistent with the manufacturer's enterprise architecture 2. Explicitly defines the authorization boundary for the system 3. Describes the operational context of the IoT device in terms of missions and business processes 4. Provides the security categorization of the IoT device, including supporting rationale 5. Describes the operational environment for the IoT device and relationships with or connections to other information systems 6. Provides an overview of the security requirements for the system 7. Identifies any relevant overlays, if applicable 8. Describes the security controls in place or planned for meeting those requirements, including a rationale for the tailoring decision 9. n/a, internal to the manufacturer b. n/a, internal to the manufacturer c. Reviews the security plan for the IoT device (assignment: organization-defined frequency) d. Updates the plan to address changes to the IoT device/environment of operation or problems identified during plan implementation or security control assessments e. Protects the security plan from unauthorized disclosure and modification
IoT-11	6	PM-11	Mission/Business Process Definition	The manufacturer of the IoT device: a. Defines mission/business processes with consideration for information security and the resulting risk to environment of use operations, manufacturer assets, individuals, other manufacturers and the nation b. Determines information protection needs arising

				from the defined mission/business processes and revises the processes as necessary until achievable protection needs are obtained
IoT-12	7	PM-1	Information Security Program Plan	The manufacturer: a. Develops and disseminates an information security program plan that: 1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements 2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among environment of use entities and compliance 3. Reflects coordination among organizational entities responsible for the different aspects of information security (e.g., technical, physical, personnel, cyberphysical) 4. Is approved by a senior official with responsibility and accountability for the risk being incurred (including mission, functions, image and reputation), manufacturer assets, individuals, other manufacturers and the nation b. Periodically (at a predefined frequency) reviews the information security program plan c. Updates the plan to address manufacturer changes and problems identified during plan implementation or security control assessments d. Protects the information security program plan from unauthorized disclosure and modification