Pre-Read Document for the NIST Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks Workshop

June 28, 2018

Table of Contents

List of Figures

List of Tables

Preface

The Internet of Things (IoT) is a rapidly evolving and expanding collection of diverse technologies that interact with the physical world. IoT devices are the outcome of combining the worlds of information technology (IT) and operational technology (OT). Many IoT devices are the result of the convergence of cloud computing, mobile computing, embedded systems, big data, low-price hardware, and other technological advances. IoT can provide computing functionality and network connectivity for equipment that previously lacked these, enabling remote control (monitoring, configuration, troubleshooting, etc.), among other features. IoT also adds the ability to analyze data about the physical world and use the results to better inform decision making, alter the physical environment, and anticipate future events.

While the full scope of IoT is not precisely defined, it is clearly vast. An incredible variety of technologies fall within the scope of IoT, ranging from smart buildings and smart manufacturing to connected vehicles and smart roads. Virtually every imaginable consumer device, many of which are also present in organizations' facilities, has become a connected IoT device—kitchen appliances, thermostats, home security cameras, door locks, light bulbs, TVs and other consumer electronics, and intelligent personal assistants. There are also many IoT devices specific to a particular sector—for example, there is an enormous IoT presence in healthcare, including hospital equipment and supplies, implantable medical devices, and wearable health monitoring equipment and fitness trackers. [1]

Many organizations are not necessarily aware they are using a large number of IoT devices. It is important that organizations understand their use of IoT because many IoT devices affect cybersecurity and privacy risks differently than IT devices do. Once organizations are aware of their existing IoT usage and possible future usage, they need to understand how the characteristics of IoT affect managing cybersecurity and privacy risks, especially in terms of risk response.

This document serves as the pre-read to help guide conversation at the Considerations for Managing IoT Cybersecurity and Privacy Risks Workshop to be held at NIST on July 11, 2018. The workshop will help NIST with the development of the Cybersecurity for IoT Program and Privacy Engineering Program's publication on an introduction to managing IoT cybersecurity and privacy risk for federal agencies. This will include work to date on identifying considerations for managing cybersecurity and privacy risk for IoT devices versus conventional IT devices, determining how those risk considerations might impact risk management in general and risk response and mitigation in particular, and identifying basic cybersecurity and privacy controls organizations may want to consider, adapt, and potentially include in their requirements when acquiring IoT devices.

This document is non-comprehensive, focusing on the aspects of cybersecurity and privacy risks where our initial analysis has found the need for more information and discussion to be greatest. Other types of risks that may be relevant for IoT devices, such as safety and reliability risks, are out of scope. **All mentions of NIST Cybersecurity Framework Subcategories, NIST Special Publication (SP) 800-53 controls, and NIST SP 800-37 tasks in this document are notional and preliminary.**

The NIST Cybersecurity for IoT Program is interested in and encourages feedback on this pre-read document, which can be provided at the workshop or to iotsecurity@nist.gov.

IoT Device Capabilities

Each IoT device provides one or more capabilities it can use on its own or in conjunction with other IoT and non-IoT devices to achieve one or more goals. For example, one IoT device may have several capabilities that work together to fully meet an objective, while another IoT device may have a single basic capability that is used by other IoT devices in order to fully meet an objective. This document references the following types of capabilities IoT devices can provide that are of primary interest in terms of potentially affecting cybersecurity and privacy risk. This is not intended to be a comprehensive list of all possible IoT device capabilities.

- *Transducer capabilities* interact with the physical world and serve as the edge between digital and physical environments. Transducer capabilities provide the ability for computing devices to interact directly with physical entities of interest. Every IoT device has at least one transducer capability. The two types of transducer capabilities are:
  - *Sensing*: the ability to provide an observation of an aspect of the physical world in the form of measurement data. Examples include temperature measurement, computerized tomography scans (radiographic imaging), optical sensing, and audio sensing.
  - *Actuating*: the ability to change something in the physical world. Examples of actuating capabilities include heating coils, cardiac electric shock delivery, electronic door locks, unmanned aerial vehicle operation, servo motors, and robotic arms.
- *Data capabilities* are typical digital computing functions: data storing, processing, and transferring. Examples of data transferring (networking) capabilities include Ethernet, Wi-Fi, Bluetooth, and Long-Term Evolution (LTE).
- *Interface capabilities* enable device interactions (e.g., device-to-device communications, human-to-device communications). The types of interface capabilities are:
  - *Application interface*: the ability for other computing devices to communicate with an IoT device through an IoT device application. An example of an application interface capability is an application programming interface (API).
  - *Human user interface*: the ability for an IoT device to communicate directly with people. Examples of human user interface capabilities include keyboards, mice, microphones, cameras, scanners, monitors, touch screens, touchpads, speakers, and haptic devices.
  - *Network interface*: the ability to interface with a communication network for the purpose of communicating data from one IoT device to another. A network interface capability allows a device to be connected to a communication network, but it does not provide the data transferring capability. Examples of network interface capabilities include Ethernet adapters, LTE radios, ZigBee radios, and Wi-Fi dongles.
- *Supporting capabilities* provide functionality that supports the other IoT capabilities. Examples are device management, cybersecurity controls, and privacy controls. [1]

Cybersecurity Risk and Privacy Risk Considerations

Cybersecurity risk and privacy risk are related but distinct concepts. *Risk* is defined in draft NIST Special Publication (SP) 800-37 Revision 2 as "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." [2] For cybersecurity, risk is about exploitation of vulnerabilities to compromise device or data confidentiality,

integrity, or availability. For privacy, risk is about *problematic data actions*—operations that process personally identifiable information (PII) through the information lifecycle and as a side effect cause individuals to experience some type of problem(s). As Figure 1 depicts, privacy and security risk overlap with respect to concerns about the security of PII, but there are also privacy concerns without implications for security, and security concerns without implications for privacy. [3]

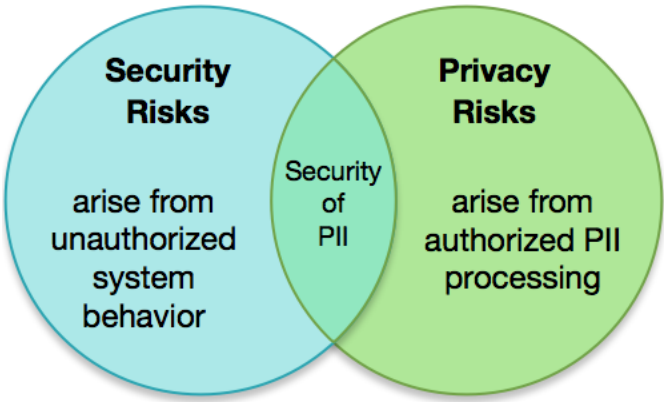

Figure 1: Relationship between Cybersecurity and Privacy Risks

IoT devices generally face the same types of cybersecurity and privacy risks as conventional IT devices, though the prevalence and severity of such risks often differ.[1] This section explores considerations that may affect the management of cybersecurity and privacy risks for IoT devices, in most cases because mitigating the risks using conventional IT controls may not be feasible or effective. Note that while each IoT device in its particular environment will have its own set of risk considerations, there are common risk considerations that can be stated at a more general level to help guide risk management.

Consideration 1: Heterogeneous Capabilities

IoT devices generally have more heterogeneous capabilities than conventional IT devices.

Conventional IT devices tend to have largely homogeneous capabilities. For example, most laptops have similar data storage, processing, and transferring capabilities; human user interface and network interface capabilities; and supporting capabilities, such as centralized management. Because the capabilities are so similar among laptops, their cybersecurity and privacy risks tend to be similar as well.

This is in contrast to IoT devices, which offer an incredible range of capabilities and combinations of those capabilities. One IoT device may have just a few basic capabilities, such as sensing data and transmitting that data to a server for processing and storage, and lack human user interfaces and centralized management capabilities. Another IoT device may include multiple sensors and actuators, use local and remote data storage and processing capabilities, and be connected to several internal and external networks at once.

[1] IoT also has implications for individuals' direct autonomy, as device operations may act upon individuals without mediation through processing PII. For example, law enforcement or other authorized third parties could take control of automated vehicles with individuals inside, or environmental controls such as lighting or temperature could be used to influence individuals' movement in buildings.

The variability in IoT device capabilities causes similar variability in the cybersecurity and privacy risks involving each IoT device. An IoT device may not need some of the controls conventional IT devices rely on—an example is an IoT device without data storage capabilities not needing to protect data at rest. An IoT device may also need additional controls that most conventional IT devices do not use, especially if the IoT device enables interactions with the physical world. Here are some examples of how that may affect cybersecurity and privacy risks:

- IoT sensor data, being based on taking measurements of the physical world, always has uncertainties associated with it. Effective management of IoT sensor data, including understanding measurement uncertainties, is necessary to avoid inadvertently introducing new risks. For many IoT devices, it is key for the organization to understand the nature of the measurements in order to assess data quality and meaning and to make decisions regarding the data's use. Without this, error rates may be unknown for the difference contexts in which an IoT device might be used.
- The ubiquity of IoT sensors in public and private environments can contribute to the aggregation and analysis of enormous amounts of data about individuals. These activities may curtail individuals' autonomy or lead to information being revealed that individuals did not anticipate or want, including the reidentification of previously de-identified PII—and may actually be well beyond the originally intended scope of the IoT device's operation.
- IoT devices with actuators have the ability to make changes to physical systems and thus affect the physical world. The potential ability to impact the physical world needs to be explicitly recognized and addressed from cybersecurity and privacy perspectives. In a worst-case scenario, a compromise could allow an attacker to use an IoT device to endanger human safety, damage or destroy equipment and facilities, or cause major operational disruptions. Privacy concerns and related civil liberties concerns could arise through authorized changes to physical systems that could impact individuals' physical autonomy or behavior in personal and public spaces. For example, law enforcement or other authorized third parties could take control of automated vehicles with individuals inside, or environmental controls such as lighting or temperature could be used to influence individuals' movement in buildings.
- IoT network interfaces often enable remote access to physical systems that previously could only be accessed locally. Vendors, manufacturers, and other third parties may be able to use remote access to IoT devices for management, monitoring, maintenance, and troubleshooting purposes. This may put the physical systems accessible through the IoT devices at much greater risk of compromise. Further, these decentralized data processing functions can exacerbate many privacy risks, making it harder for individuals to develop reliable assumptions and participate in decision making about the processing of their information.

IoT device interactions with the physical world may also have an impact on how certain controls are used because of the risk those controls themselves can introduce. Practices such as patching are generally considered essential for conventional IT, but these practices could have far greater negative impacts on some IoT devices with actuators, making critical services unavailable and endangering human safety. Configuring these IoT devices to automatically download and install patches could be dangerous. An organization might reasonably decide that patches should be installed manually at a date and time chosen by the organization with the appropriate staff onsite and ready to react immediately if a problem occurs. An organization might also reasonably decide to avoid patching certain IoT devices

altogether and instead tightly restrict logical and physical access to them to prevent exploitation of unpatched vulnerabilities.

Consideration 2: Lack of Device Access, Management, and Monitoring Features

Many IoT devices cannot be accessed, managed, or monitored in the same ways conventional IT devices can.

Conventional IT devices usually provide authorized people, processes, and devices with hardware and software access, management, and monitoring features. In other words, an authorized administrator, device, or process can directly access a conventional IT device's firmware, operating system, and applications, fully manage the device and its software as needed, and monitor the internal characteristics and state of the device at all times. Authorized users can also access a restricted subset of the access, management, and monitoring features.

In contrast, many IoT devices are inflexible and opaque, often referred to as "black boxes". They provide little or no visibility into their state and composition, and little or no access to and management of their software and configuration. In extreme cases, it may be difficult to determine if a black box product is actually an IoT device because of the lack of information.

Authorized people, devices, and processes may encounter one or more of the following challenges in accessing, managing, monitoring, and using IoT devices that affect cybersecurity and privacy risk:

- **Lack of management features.** Administrators may not be able to fully manage an IoT device's firmware, operating system, and applications. Unavailable features may include the ability to acquire, verify the integrity of, install, configure, store, retrieve, execute, terminate, remove, and replace or update software. In addition, an IoT device's software may be automatically reconfigured when an adverse event occurs, such as a power failure or a loss of network connectivity.
- **Lack of interfaces.** Some IoT devices lack application and/or human user interfaces for device use and management. When such interfaces do exist, they may not provide the functionality usually offered by IT devices. An example is the challenge in notifying users about an IoT device's processing of their PII so they provide meaningful consent to this processing. An additional issue is the lack of universally accepted standards for IoT application interfaces, including expressing and formatting data, issuing commands, and otherwise fostering interoperability between IoT devices.
- **Difficulties with management at scale.** Most IoT devices do not support standardized mechanisms for centralized management, and the sheer number of IoT devices to be managed may be overwhelming.
- **Wide variety of software to manage.** There is extensive variety in the software used by IoT devices, including firmware, standard and real-time operating systems, and applications. This significantly complicates software management throughout the IoT device lifecycle, affecting such areas as configuration and patch management.
- **Differing lifespan expectations.** A manufacturer may intend for a particular IoT device to only be used for three to five years and then discarded. An organization purchasing that product might want to use it for ten years or more, but the manufacturer may stop supporting the product (e.g., releasing patches for known vulnerabilities).

- **Unserviceable hardware.** IoT device hardware may not be serviceable, meaning it cannot be repaired, customized, or inspected internally.
- **Lack of inventory capabilities.** IoT devices brought into an organization may not be inventoried, registered, and otherwise provisioned via the normal IT processes.
- **Heterogeneous ownership.** There is often heterogeneous ownership of IoT devices. For example, an IoT device may transfer data to vendor-provided cloud-based service processing and storage because the IoT device lacks these processing and storage capabilities. Data may also be sent to a cloud service to aggregate data from multiple IoT devices in a single location. These cloud services may have access to portions or all of the devices' data, or even access to and control of the devices themselves for monitoring, maintenance, and troubleshooting purposes. In some cases, only vendors have the authority to do maintenance; an organization attempting to install patches or do other maintenance tasks on an IoT device may void its warranty. Also, in IoT there may be little or no information available about device ownership, especially in black box IoT devices. This could exacerbate existing privacy redress difficulties because the lack of accountability limits individuals' abilities to locate the source of and correct or delete inaccurate information about themselves, or to address other problems.

Consideration 3: Control Availability, Efficiency, and Effectiveness

The availability, efficiency, and effectiveness of cybersecurity and privacy controls is often different for IoT devices than conventional IT devices.

For the purposes of this document, built-in cybersecurity and privacy controls are called *pre-market controls*. Pre-market controls are integrated into IoT devices by the manufacturer or vendor before they are shipped to customer organizations. *Post-market controls* are those controls that organizations select, acquire, and deploy themselves in addition to pre-market controls. Pre-market and post-market cybersecurity and privacy controls are often different for IoT devices than conventional IT. The main reasons for this are:

- **Unavailable controls.** Many IoT devices do not or cannot support the range of controls typically built into conventional IT products. For example, a "black box" IoT device may not log its cybersecurity and privacy events or may not give organizations access to its logs. Only certain types of cryptography have privacy-enhancing features that limit exposure of individuals' data trails even among authorized parties. If pre-market controls are available for IoT devices, they may be inadequate in terms of strength or performance—for example, using strong encryption and mutual authentication to protect communications may cause unacceptable delays. Post-market controls cannot be installed onto many IoT devices. Also, existing pre-market and post-market controls may not be able to scale to meet the needs of IoT—the number of devices, the volume of network traffic and generated data, etc.
- **Inefficient controls.** The level of effort needed to manage, monitor, and maintain pre-market controls may be excessive. Especially when IoT devices do not have robust capabilities for centralized management, it may be more efficient to implement and use centralized post-market controls that each help protect numerous IoT devices instead of trying to achieve the equivalent level of protection on each individual IoT device. One example is having a single network-based IoT gateway or IoT security gateway protecting many IoT devices instead of having to design, manage, and maintain a unique set of controls within each IoT device.

- **Ineffective controls.** Some post-market controls, such as network-based intrusion prevention systems, antimalware servers, and firewalls, may not be as effective at protecting IoT devices as they are at protecting conventional IT. IoT devices often use protocols that conventional IT controls cannot understand and analyze. Also, IoT devices may communicate directly with each other, such as through point-to-point wireless communication, instead of using a monitored infrastructure network.

Organization-Level Cybersecurity and Privacy Risk Considerations

Organizations should already be addressing cybersecurity and privacy risk considerations for IoT devices throughout the IoT device lifecycle in their existing cybersecurity and privacy policies, plans, programs, and processes. Organizations can ensure they have clearly and formally stated the definition or scope of IoT they will use in order to avoid confusion and ambiguity. This is particularly important if an organization is subject to multiple laws, regulations, or other external requirements for IoT cybersecurity or privacy that have different IoT definitions and scopes.

Similarly, organizations can ensure their cybersecurity, supply chain, and privacy risk management programs take IoT into account appropriately. This includes the following:

- Identifying IoT device capabilities. Know which types of IoT devices are in use, which capabilities each type supports, and what purpose each capability helps provide.
- Assessing IoT device risk. It is important to take into consideration the particular IoT environment the IoT devices reside within, and not just assess risks for IoT devices in isolation. For example, attaching an actuator to one physical system may affect risks much differently than attaching the same actuator to another physical system.
- Determining how to respond to that risk by accepting, avoiding, mitigating, sharing, or transferring it. As previously discussed, some risk mitigation strategies for conventional IT may not work well for IoT.

Organizations can ensure their CSF usage takes IoT into account, especially for the following CSF Subcategories [4]:

- ID.BE (Identify—Business Environment)
  - ID.BE-4: Dependencies and critical functions for delivery of critical services are established
  - ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)
- ID.GV (Identify—Governance)
  - ID.GV-1: Organizational cybersecurity policy is established and communicated
  - ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners
  - ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
  - ID.GV-4: Governance and risk management processes address cybersecurity risks
- ID.RA (Identify—Risk Assessment)
  - ID.RA-1: Asset vulnerabilities are identified and documented
  - ID.RA-3: Threats, both internal and external, are identified and documented
  - ID.RA-4: Potential business impacts and likelihoods are identified

    - ID.RA-6: Risk responses are identified and prioritized
- ID.RM (Identify—Risk Management Strategy)
    - ID.RM-2: Organizational risk tolerance is determined and clearly expressed
    - ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis
- ID.SC (Identify—Supply Chain Risk Management)
    - ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process
    - ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.
- PR.IP (Protect—Information Protection Processes and Procedures)
    - PR.IP-3: Configuration change control processes are in place
    - PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
    - PR.IP-12: A vulnerability management plan is developed and implemented

Organizations can ensure their draft NIST SP 800-37 Revision 2 [2] usage takes IoT privacy risk considerations into account, especially for the tasks listed below. Note that although the CSF can be used to manage the PII cybersecurity aspect of privacy, NIST SP 800-37 Revision 2 can be used to manage the full scope of privacy because it integrates authorized PII processing into the NIST Risk Management Framework.

- Prepare, Organization Level, Task 1: Risk Management Roles
- Prepare, Organization Level, Task 2: Risk Management Strategy
- Prepare, Organization Level, Task 3: Risk Assessment—Organization
- Prepare, System Level, Task 1: Mission or Business Focus
- Prepare, System Level, Task 8: Protection Needs—Security and Privacy Requirements

Device-Level Cybersecurity Risk Mitigation

This section discusses how the risk considerations affect mitigating cybersecurity risk for IoT devices—in other words, how mitigation options differ for IoT versus conventional IT. The purpose of this section is to help organizations make better-informed decisions about how to respond to risk. This section is not intended to be comprehensive. It covers the following areas of cybersecurity risk mitigation thought to be most significantly or unexpectedly affected by the risk considerations:

- Asset management: maintain a current, accurate inventory of all IoT devices and their relevant characteristics throughout the devices' lifecycles in order to use that information for cybersecurity and privacy risk management purposes.
- Vulnerability management: identify and eliminate known vulnerabilities in IoT device software and firmware in order to reduce the likelihood of exploitation and compromise.
- Access management: prevent unauthorized and improper physical and logical access to, usage of, and administration of IoT devices by people, processes, and other computing devices.

- Data protection: prevent access to and tampering with data at rest or in transit that might expose sensitive information or allow manipulation or disruption of IoT device operations.
- Incident detection and handling: monitor and analyze activity involving IoT devices for signs of security incidents, then handle those incidents to minimize their impact.

Table 1 lists the elements from these areas that are most likely to be affected by cybersecurity risk considerations. For each element, the second column of the table lists closely related CSF Subcategories, and the third column lists closely related NIST draft SP 800-53 Revision 5 controls [5]. **The table is notional and includes selected examples; it does not define or imply any mapping or other relationship between the CSF Subcategories and the SP 800-53 controls.**

Table 1: Affected Cybersecurity Risk Mitigation Elements

Element	CSF Subcategories	SP 800-53 Controls
1. Asset identification	• ID.AM-1: Physical devices and systems within the organization are inventoried • ID.AM-4: External information systems are catalogued • PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	• AC-20, Use of External Systems • CM-8, System Component Inventory
2. Asset characterization	• ID.AM-2: Software platforms and applications within the organization are inventoried • PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	• CM-8, System Component Inventory
3. Asset tracking	• PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	• CM-8, System Component Inventory
4. Patch and upgrade management	• PR.IP-12: A vulnerability management plan is developed and implemented	• SI-2, Flaw Remediation
5. Configuration management	• PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality) • PR.IP-3: Configuration change control processes are in place • PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	• CM-2, Baseline Configuration • CM-3, Configuration Change Control • CM-6, Configuration Settings • CM-7, Least Functionality • SC-42, Sensor Capability and Data
6. Vulnerability identification	• DE.CM-8: Vulnerability scans are performed	• RA-5, Vulnerability Scanning
7. User, device, and process identity and credential management	• PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	• IA-4, Identifier Management • IA-5, Authenticator Management

Element	CSF Subcategories	SP 800-53 Controls
8. User, device, and process identity and credential usage (authentication)	• PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes • PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	• AC-7, Unsuccessful Logon Attempts • AC-11, Device Lock • AC-12, Session Termination • IA-2, Identification and Authentication (Organizational Users) • IA-3, Device Identification and Authentication • IA-6, Authenticator Feedback • IA-8, Identification and Authentication (Non-Organizational Users) • IA-9, Service Identification and Authentication • IA-11, Re-Authentication
9. Physical access authorization	• PR.AC-2: Physical access to assets is managed and protected • PR.PT-2: Removable media is protected and its use restricted according to policy	• MP-2, Media Access • MP-7, Media Use • PE-3, Physical Access Control
10. Logical access authorization (both local and remote logical access)	• PR.AC-3: Remote access is managed • PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties • PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation) • PR.DS-5: Protections against data leaks are implemented • PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools • PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	• AC-3, Access Enforcement • AC-4, Information Flow Enforcement • AC-5, Separation of Duties • AC-6, Least Privilege • AC-17, Remote Access • SC-7, Boundary Protection

Element	CSF Subcategories	SP 800-53 Controls
11. Logical protection of stored data	• PR.DS-1: Data-at-rest is protected • PR.IP-4: Backups of information are conducted, maintained, and tested • PR.IP-6: Data is destroyed according to policy • PR.PT-2: Removable media is protected and its use restricted according to policy	• AC-20, Use of External Systems • CP-9, System Backup • MP-4, Media Storage • MP-6, Media Sanitization • SC-28, Protection of Information at Rest
12. Logical protection of network communications	• PR.DS-2: Data-in-transit is protected	• AC-18, Wireless Access • AC-20, Use of External Systems • SC-8, Transmission Confidentiality and Integrity • SC-23, Session Authenticity
13. Event monitoring	• DE.AE-3: Event data are collected and correlated from multiple sources and sensors • DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed • PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	• AU-2, Audit Events • AU-3, Content of Audit Records • AU-5, Response to Audit Processing Failures • AU-6, Audit Review, Analysis, and Reporting • AU-12, Audit Generation • SI-4, System Monitoring
14. Incident detection and analysis	• DE.CM-1: The network is monitored to detect potential cybersecurity events • DE.CM-4: Malicious code is detected • PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity • RS.AN-1: Notifications from detection systems are investigated • RS.AN-3: Forensics are performed	• IR-4, Incident Handling • SI-3, Malicious Code Protection • SI-4, System Monitoring • SI-7, Software, Firmware, and Information Integrity

Table 2 lists common assumptions for the pre-market controls used to implement the Table 1 elements for conventional IT devices. For each assumption, Table 2 defines one or more possible challenges IoT devices may pose to the assumption. Next to each challenge is the NIST SP 800-53 controls from Table 1 that may be negatively affected, the potential implications of each challenge, and the CSF Subcategories from Table 1 that may be negatively affected. **Table 2 is notional and includes selected examples; it does not define or imply any mapping or other relationship between the SP 800-53 controls and the CSF Subcategories.**

Table 2: IoT Challenges to Conventional IT Pre-Market Control Assumptions

Challenges in IoT Devices	SP 800-53 Controls	Potential Implications	CSF Subcategories
Assumption 1: The product has a built-in unique identifier.			
1. The IoT device may not have a unique identifier that the organization's asset management system can access or understand.	CM-8	• May complicate device management, including remote access and vulnerability management.	ID.AM-1
Assumption 2: The product can interface with enterprise asset management systems.			
2. The IoT device may not be able to participate in a centralized asset management system.	CM-8	• May have to use multiple asset management systems. • May have to perform asset management tasks manually.	ID.AM-1 ID.AM-2 PR.DS-3
3. The IoT device may not be directly attached to any of the organization's networks.	CM-8	• May have to use a separate asset management system or service, or manual asset management processes, for external IoT devices.	ID.AM-1 ID.AM-2 PR.DS-3
Assumption 3: The product can provide the organization reasonable visibility into its characteristics.			
4. The IoT device may be a black box that provides little or no information on its hardware, software, and firmware.	CM-8	• May complicate all aspects of device management and risk management.	ID.AM-1 ID.AM-2 ID.AM-4
Assumption 4: The product or the product's manufacturer can inform the organization of all external software and services the product uses, such as software running on or dynamically downloaded from the cloud.			
5. Not all of the IoT device's external dependencies may be revealed.	AC-20	• Cannot manage risk for the external software and services.	DE.CM-8 PR.IP-1 PR.PT-3
Assumption 5: The manufacturer will provide patches or upgrades for all software and firmware throughout each product's lifespan.			
6. The manufacturer may not release patches or upgrades for the IoT device.	SI-2	• Cannot remove known vulnerabilities in the IoT device.	PR.IP-1
7. The manufacturer may stop releasing patches and upgrades for the IoT device while it is still in use.	SI-2	• May not be able to remove known vulnerabilities in the IoT device in the future.	PR.IP-1
Assumption 6: The product either has its own secure built-in patch, upgrade, and configuration management capabilities, or can interface with enterprise vulnerability management systems with such capabilities.			
8. The IoT device may not be capable of having its software patched or upgraded.	SI-2	• Cannot remove known vulnerabilities in the IoT device.	PR.IP-1

Challenges in IoT Devices	SP 800-53 Controls	Potential Implications	CSF Subcategories
9. It may be too risky to install patches or upgrades or to make configuration changes without extensive testing and preparation first, and implementing changes may require operational outages or inadvertently cause outages.	CM-3 CM-6 SI-2	• Removing known vulnerabilities may be significantly delayed.	PR.IP-1
10. The IoT device may not be able to participate in a centralized vulnerability management system.	CM-3 SI-2	• May have to use numerous vulnerability management systems instead of one. • May have to perform vulnerability management tasks manually and periodically (e.g., manually install patches, manually check for software configuration errors).	PR.IP-1
11. The IoT device may not offer the ability to change the software configuration or may not offer the features organizations want.	CM-2 CM-3 CM-6 CM-7 SC-42	• Cannot remove known vulnerabilities in the IoT device. • Cannot achieve the principle of least functionality by disabling unneeded services, functions. • Cannot restrict sensor activation and usage.	PR.IP-1 PR.IP-3 PR.PT-3
Assumption 7: The product either supports the use of vulnerability scanners or provides built-in vulnerability identification and reporting capabilities.			
12. There may not be a vulnerability scanner that can run on or against the IoT device.	RA-5	• Cannot automatically identify known vulnerabilities in the IoT device.	DE.CM-8
13. The IoT device may not offer any built-in capabilities to identify and report on known vulnerabilities.	RA-5	• Cannot automatically identify known vulnerabilities in the IoT device.	DE.CM-8
Assumption 8: The product can uniquely identify each user, device, and process attempting to logically access it.			
14. The IoT device may not support any use of identifiers.	IA-2 IA-3 IA-4 IA-8 IA-9	• Cannot identify or authenticate users, devices, and processes.	PR.AC-1 PR.AC-7

Challenges in IoT Devices	SP 800-53 Controls	Potential Implications	CSF Subcategories
15. The IoT device may only support the use of one or more shared identifiers.	IA-2 IA-3 IA-4 IA-8 IA-9	• Cannot uniquely identify users, devices, and processes. Complicates credential management because of shared credentials.	PR.AC-1
16. The IoT device may require the use of identifiers but only in certain cases (for example, for remote access but not local access, or for administration purposes but not regular usage).	IA-2 IA-3 IA-4 IA-8 IA-9	• Cannot identify or authenticate some users, devices, and processes.	PR.AC-1 PR.AC-7
Assumption 9: The product can conceal password characters from display when a person enters a password for a product, such as on a keyboard or touch screen.			
17. The IoT device may not support concealment of displayed password characters.	IA-6	• Increases the likelihood of credential theft.	PR.AC-7
Assumption 10: The product can authenticate each user, device, and process attempting to logically access it.			
18. The IoT device may not support use of non-trivial credentials (e.g., does not support the use of identifiers, does not allow default passwords to be changed).	IA-5	• Cannot identify or authenticate users, devices, and processes.	PR.AC-7
19. The IoT device may not support the use of strong credentials, such as cryptographic tokens or multifactor authentication, for the situations that merit them.	IA-5	• Increases the chances of unauthorized access through credential misuse.	PR.AC-7
Assumption 11: The product can use existing enterprise authenticators and authentication mechanisms.			
20. The IoT device may not support the use of an existing enterprise user authentication system.	IA-2 IA-5 IA-8	• Need one or more additional accounts and credentials for each user.	PR.AC-1 PR.AC-7
Assumption 12: The product can restrict each user, device, and process to the minimum logical access privileges necessary.			
21. The IoT device may not support use of logical access privileges within the device that is sufficient for a given situation.	AC-3 AC-5 AC-6	• Allows authorized users, devices, and processes to intentionally or inadvertently use privileges they should not have. • Allows an attacker who gains unauthorized access to an account to have greater access to the device.	PR.AC-4 PR.DS-5 PR.MA-1

Challenges in IoT Devices	SP 800-53 Controls	Potential Implications	CSF Subcategories
22. The IoT device may not support use of logical access privileges to restrict network communications into and out of the device that is sufficient for a given situation.	AC-3 AC-4 AC-5 AC-6 AC-17 SC-7	• Allows authorized users, devices, and processes to intentionally or inadvertently conduct network communications they should not be able to. • Allows an attacker to have greater network access to the device than intended.	PR.AC-3 PR.AC-5 PR.DS-5 PR.MA-2
Assumption 13: The product can thwart attempts to gain unauthorized access, and this feature can be configured or disabled to avoid undesired disruptions to availability. (Examples include locking or disabling an account when there are too many consecutive failed authentication attempts, delaying additional authentication attempts after failed attempts, and locking or terminating idle sessions.)			
23. The IoT device's use of these security features may not be sufficiently modifiable.	AC-7 AC-11 AC-12 IA-11	• Cannot gain immediate access to an IoT device when needed to use or manage it.	PR.AC-3 PR.AC-4 PR.MA-1 PR.MA-2
Assumption 14: The product has adequate built-in physical security controls to protect it from tampering (e.g., tamper-resistant packaging).			
24. The IoT device may be deployed in an area where people who are not authorized to access the device may do so or where authorized people can access the device in unauthorized ways.	MP-2 MP-7 PE-3	• Allows an attacker to have direct physical access to the device and tamper with it, including adding or removing storage media, connecting peripherals, etc.	PR.AC-2 PR.PT-2 PR.MA-1
Assumption 15: The product can prevent unauthorized access to all sensitive data on its storage devices.			
25. The IoT device may not provide sufficiently strong encryption capabilities for its stored data.	AC-20 MP-4 SC-28	• Increased likelihood of unauthorized access to sensitive data.	PR.DS-1 PR.PT-2
26. The IoT device may not provide a mechanism for sanitizing sensitive data before disposing of or repurposing the device.	MP-6	• Increased likelihood of unauthorized access to sensitive data.	PR.IP-6
Assumption 16: The product has a mechanism to support data availability through secure backups.			
27. The IoT device may not provide a secure backup and restore mechanism for its data.	CP-9	• Increased likelihood of loss of data.	PR.IP-4

Challenges in IoT Devices	SP 800-53 Controls	Potential Implications	CSF Subcategories
Assumption 17: The product can prevent unauthorized access to all sensitive data transmitted from it over networks.			
28. The IoT device may not provide sufficiently strong encryption capabilities for protecting sensitive data sent in its network communications.	AC-18 AC-20 SC-8	• Increased likelihood of eavesdropping on communications.	PR.DS-2
29. The IoT device may not verify the identity of another computing device before sending sensitive data in its network communications.	SC-8 SC-23	• Increased likelihood of eavesdropping, interception, manipulation, impersonation, and other forms of attack on communications.	PR.DS-2
Assumption 18: The product can log its operational and security events.			
30. The IoT device may not be able to log its operational and security events at all or in sufficient detail.	AU-2 AU-3 AU-12 SI-4	• Increased likelihood of malicious activity going undetected. • Inability to confirm and reconstruct incidents from log entries.	DE.CM-7 PR.PT-1 RS.AN-1
31. The IoT device may continue operating even when a logging failure occurs.	AU-5	• Increased likelihood of malicious activity going undetected.	DE.CM-7 PR.PT-1
Assumption 19: The product can interface with existing enterprise log management systems.			
32. The IoT device may not be able to participate in an enterprise log management system.	AU-6 SI-4	• May have to use numerous log management systems instead of one. • May have to perform log management tasks manually. • Increased likelihood of malicious activity going undetected	DE.AE-3 DE.CM-7 PR.PT-1
Assumption 20: The product can facilitate the detection of potential incidents by internal or external controls, such as intrusion prevention systems, anti-malware utilities, and file integrity checking mechanisms.			
33. The IoT device may not be able to execute internal detection controls or interact with external detection controls without adversely affecting device operation.	SI-3 SI-7	• Increased likelihood of malicious code infections and other unauthorized activities occurring and going undetected.	DE.CM-1 DE.CM-4 PR.DS-6
34. The IoT device may not provide controls with the visibility needed to detect incidents efficiently and effectively.	IR-4	• Increased likelihood of malicious code and other unauthorized activities going undetected.	DE.CM-1 DE.CM-4 PR.DS-6

Challenges in IoT Devices	SP 800-53 Controls	Potential Implications	CSF Subcategories
Assumption 21: The product can support event and incident analysis activities.			
35. The IoT device may not provide analysts with sufficient access to the device's resources in order to do the necessary analysis.	SI-4	• Inability to use forensic tools for information gathering and analysis.	RS.AN-1 RS.AN-3

Device-Level Privacy Risk Mitigation

This section discusses how the risk considerations affect mitigating privacy risk arising from authorized PII processing for IoT devices—in other words, how mitigation options differ for IoT versus conventional IT. The purpose of this section is to help organizations make better-informed decisions about how to respond to risk in order to achieve their privacy objectives for IoT.

This section is not intended to be comprehensive. It focuses on the areas of privacy risk mitigation thought to be most significantly or unexpectedly affected by the IoT risk considerations. Since this section focuses on privacy risk arising from authorized PII processing, CSF outcomes are not addressed. However, organizations may use the section on device-level cybersecurity risk mitigation to address privacy risks arising from the loss of confidentiality, integrity, or availability of PII.

Many existing privacy controls and requirements reflect privacy principles that are based on underlying assumptions about management of PII largely through interconnected databases under clearly identifiable ownership or control and the resulting capabilities for individual engagement with these types of devices. The application of these principles has not been straightforward even in conventional IT devices; however, the complexity, dynamic nature, decentralized data processing functions, lack of accustomed interfaces, and heterogenous ownership or control of IoT devices are likely to exacerbate the difficulties organizations face in applying customary privacy controls.

These difficulties highlight the importance of taking a more outcome- and risk-based approach to managing privacy for IoT. The NIST privacy engineering objectives—predictability, manageability, and disassociability—support the development of an outcome-based approach by focusing on the properties systems should deliver as a whole. [3] Privacy principles, rather than being treated as a checklist of requirements, can be used to inform the rationale for how and why to build IoT devices that support the ability for individuals to balance their autonomy with societal engagement. For example, considering how to disassociate data from individuals or devices while still permitting functionality in the IoT devices could lead to overall changes in design that mitigate privacy risk and organically meet the goal of the data minimization principle. Analyzing where privacy risks are arising (i.e., which data actions are likely to create problems for individuals and the impact if they occur) in the particular context of how the IoT devices are functioning can be taken into account rather than trying to apply data minimization at a general level.

Table 3 lists the privacy controls for conventional IT from draft NIST SP 800-53 Revision 5 that are most likely to be affected by one or more IoT privacy risk considerations. Organizations can select compensating controls to augment or take the place of inadequate or missing pre-market controls, and implement those compensating controls to reduce privacy risk for individuals.

Table 3: NIST SP 800-53 Controls Affected by IoT Privacy Risk Considerations

Possible Challenges in IoT Environments	Affected SP 800-53 Controls	Implications
Assumption 22: The product operates in a traditional federated identity environment.		
36. The IoT device may contribute data that is used for identification and authentication, but is outside of traditional federated environments.	IA-8 (6), Identification and Authentication (non-organizational users) | Disassociability	Techniques such as the use of identifier mapping tables and privacy-enhancing cryptographic techniques to blind credential service providers and relying parties from each other or to make identity attributes less visible to transmitting parties may not work outside a traditional federated environment.
Assumption 23: Traditional interfaces exist for individual engagement with the product.		
37. The IoT device may lack interfaces that enable individuals to interact with it.	IP-2, Consent	Individuals may not be able to provide consent to the processing of their PII or condition further processing of specific attributes.
38. Decentralized data processing functions and heterogenous ownership of IoT devices challenge traditional accountability processes.	IP-3, Redress	Individuals may not be able to locate the source of inaccurate or otherwise problematic PII in order to correct it or fix the problem.
39. The IoT device may lack interfaces that enable individuals to read privacy notices.	IP-4, Privacy Notice	Individuals may not be able to read or access privacy notices.
40. The IoT device may lack interfaces to enable access to PII, or PII may be stored in unknown locations.	IP-6, Individual Access	Individuals may have difficulty accessing their information, which curtails their ability to manage their information and understand what is happening with their data, and increases compliance risks.
Assumption 24: There is sufficient centralized control to apply policy or regulatory requirements to PII.		
41. The IoT device may collect PII indiscriminately or analyze, share or act upon the PII based on automated processes.	PA-2, Authority to Collect	PII may be processed in ways that are out of compliance with regulatory requirements or an organization's policies.
42. IoT devices may be complex and dynamic with sensors being frequently added and removed.	PA-3, Purpose Specification	PII may be hard to track such that individuals, as well as device owners/operators, may not have reliable assumptions about how PII is being processed, making it difficult to make informed decisions.
43. The IoT device may be accessed remotely allowing the sharing of PII outside the control of the administrator	PA-4, Information Sharing with External Parties	PII may be shared in ways that are out of compliance with regulatory requirements or an organization's policies.

Possible Challenges in IoT Environments	Affected SP 800-53 Controls	Implications
Assumption 25: There is sufficient centralized control to manage PII.		
44. IoT devices may be complex and dynamic with sensors being frequently added and removed.	PM-29, Inventory of Personally Identifiable Information	PII may be difficult to identify and track using traditional inventory methods.
45. IoT devices may not support standardized mechanisms for centralized data management, and the sheer number of IoT devices to manage may be overwhelming.	SC-7 (24), Boundary Protection | Personally Identifiable Information	Application of PII processing rules intended to protect individuals' privacy may be disrupted.
46. The IoT device may not have the capability to support configurations such as preventing remote activation, limited data reporting, notice of collection, and data minimization.	SC-42, Sensor Capability and Data	Lack of direct privacy risk mitigation capabilities may require compensating controls and may impact an organization's ability to optimize the amount of privacy risk that can be reduced.
47. The IoT device may indiscriminately collect PII. Heterogenous ownership of devices challenge traditional data management techniques.	SI-12 (1), Information Management and Retention | Limit Personally Identifiable Information Elements	Increased likelihood that operationally unnecessary PII will be retained.
48. Decentralized data processing functions and heterogenous ownership of IoT devices challenge traditional data management processes with respect to checking for accuracy of data.	SI-19, Data Quality Operations	Increased likelihood that inaccurate PII will persist with the potential to create problems for individuals.
49. Decentralized data processing functions and heterogenous ownership of IoT devices challenge traditional de-identification processes.	SI-20, De-Identification	Aggregation of disparate data sets may lead to re-identification of PII.

Control Sets, Baselines, and Overlays

Most efforts to date applying IoT device cybersecurity and privacy controls for industry, consumers, and others have focused on specifying the pre-market controls manufacturers should incorporate into the IoT devices they design and build. Although this is important and helpful, organizations are already using many IoT devices without these controls, and it will take time for manufacturers to improve their pre-market controls, if that can be done without making the products too costly. Organizations also need to

be mindful of IoT manufacturers no longer supporting their older products or going out of business altogether. Deployed IoT devices have a range of cybersecurity and privacy pre-market controls in place; these pre-market controls vary from device to device. Some IoT devices were designed to allow for updates while deployed, and others are not. Organizations may already have IoT devices in place with cybersecurity and privacy controls implemented, or may have IoT devices in place with no pre-market controls implemented.

Accordingly, our work focuses on cybersecurity and privacy risks for IoT devices that lack the full range of robust pre-market controls. There has been interest from the private sector in having a single set of cybersecurity and privacy controls that organizations could apply to all their IoT devices, including those lacking pre-market controls. Unfortunately, each of the three considerations defined earlier in this document negatively impacts the feasibility of having a single control set. To recap the considerations:

1. IoT devices generally have more heterogeneous capabilities than conventional IT devices.
2. Many IoT devices cannot be accessed, managed, or monitored in the same ways conventional IT devices can.
3. The availability, efficiency, and effectiveness of cybersecurity and privacy controls is often different for IoT devices than conventional IT devices.

Given the variety of IoT device capabilities, the issues with accessing, managing, and monitoring IoT devices, and the problems with implementing and using many cybersecurity and privacy controls for IoT devices, it is not possible to define a single control set for all of IoT. In NIST SP 800-53 terminology, it is not feasible to define a single control overlay for all IoT devices for federal agencies to use to tailor the NIST SP 800-53 control baselines. An overlay is “a specification of security or privacy controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines.” [5] We plan on investigating the possibility of defining groups of compensating controls to serve as NIST SP 800-53 overlays for federal agencies, with each overlay addressing a specific subset of IoT devices.

It is also not feasible to state all acceptable alternatives to augment or take the place of weak or missing pre-market controls, especially when many IoT devices are controlled partially or completely by vendors, manufacturers, and other third parties. Addressing risks for those devices may involve the use of altogether different risk response strategies, such as having the third parties sign service level agreements (SLAs) defining requirements they must meet for the IoT devices they manage. Organizations may also want to use additional controls to help reduce the impact of any failures or misuse of third party-managed devices based on the organization’s risk tolerance.

Some mitigation problems can potentially be addressed by using post-market compensating controls instead of pre-market controls. However, current post-market controls may not be as effective as expected or needed for IoT devices. Different post-market controls may be needed to supplement or take the place of existing post-market controls, and altogether different post-market control strategies may be needed. Over time, post-market controls are likely to be improved to better handle IoT, but organizations may need to find other ways to mitigate risk in the meantime.

For example, if removing vulnerabilities from a group of IoT devices is not feasible, an organization could instead focus its resources on preventing attackers and attacks from reaching the vulnerable devices in the first place. This could be achieved by using a combination of physical and logical access controls to

restrict access, along with network-based controls that carefully examine the contents of incoming network traffic and block all traffic that is not specifically authorized or that appears to have malicious intent. However, the more restrictive controls are, the more likely it is that benign activity will inadvertently be blocked. For example, during an emergency you might have a third party helping with troubleshooting who normally does not have access. Also, if all protection occurs through access controls, an access control failure may make it trivial for attackers to exploit vulnerabilities and compromise IoT devices.

Likewise, with respect to post-market privacy controls, where IoT devices may lack conventional user interfaces to provide notices or obtain consent, organizations may consider how the NIST privacy engineering objectives (like predictability) can expand outcomes for organizations. [3] For example, when considering how to enable reliable assumptions about what the IoT devices are collecting in the absence of traditional notice and consent interfaces, organizations may consider applying differential privacy techniques to the PII as it comes through the devices; this could limit what information is being revealed that individuals might not have anticipated.

Table 4 provides examples of possible compensating controls for cybersecurity and privacy risk mitigation, along with which challenges from Table 2 each example addresses at least partially.

Table 4: Examples of Possible Compensating Controls

Example of Possible Compensating Control	Challenges Addressed
Asset Management	
Monitor network traffic to identify the IoT device's interactions with external systems and the nature of each interaction.	5
Manually review the IoT device's characteristics by using operating system access.	4 and 5
Vulnerability Management	
Use access management pre-market and post-market controls instead of vulnerability management controls.	Reduces importance of 6 through 13
Disable vulnerable IoT device features that are deemed too risky.	Reduces importance of 6 through 13
Access Management	
Use a remote access security technology to uniquely authenticate users, devices, and processes before granting them remote access to the IoT device.	14, 15, 16, 18, 19, 20, 23
Use an IoT gateway or security gateway to restrict which actions involving the IoT device are permitted over networks.	21, 22
Use physical security measures to compensate for the lack of local logical security controls.	14, 16, 17, 18, 24
Use network segmentation to isolate IoT devices from other devices.	14, 18, 22
Data Protection	
Configure the IoT device so it does not collect sensitive data that is not needed or cannot be adequately protected.	Reduces importance of 25 through 29

Example of Possible Compensating Control	Challenges Addressed
Configure the IoT device so it does not store sensitive data it collects.	Reduces importance of 25, 26, and 27
Configure the IoT device so it does not transmit sensitive data.	Reduces importance of 28
Use VPN technology to provide an encrypted tunnel for transmitted sensitive data and to authenticate both endpoints before establishing a tunnel between them.	28, 29
Incident Detection and Handling	
Use an IoT security gateway, network-based intrusion prevention system, or other network-based security control to log security events and detect possible incidents. May need to alter where traffic encryption/decryption occurs within the network in order for this to work. May need to route network traffic through these devices.	30 through 35
Rely more on access management, vulnerability management, and data protection controls to prevent incidents than incident detection and handling controls.	Reduces importance of 30 through 35
Privacy	
Provide notices and consent mechanisms independent of the IoT device.	37, 39, 40
Use data tags to enable automated means of locating PII and managing PII processing permissions.	38, 41, 42, 43, 44, 45, 47, 48; indirectly 49
Apply policy requirements such as disposing of unnecessary PII after collection.	Reduces importance of 46
Apply policy requirements about the combining of data sets and/or re-identification prohibitions.	49

Possible Pre-Market Controls for IoT Device Acquisitions

As discussed earlier in this document, some risk considerations can be wholly or partially addressed by IoT device manufacturers through pre-market controls. For example, a manufacturer could design and produce an IoT device so it is capable of logging its internal security events and making those logs accessible to authorized administrators. Without this built-in capability, organizations acquiring the device might not have any way of monitoring its internal security events.

This section proposes a list of pre-market cybersecurity and privacy controls that organizations may want to consider, adapt, and potentially include in their requirements when acquiring IoT devices. As noted in earlier sections, some controls may not be needed for particular situations, or other pre-market or post-market compensating controls may adequately take their place. Many other controls not in this section may also be needed. The controls listed in this section are intended as a starting point for consideration**; they do not define or imply any mapping or other relationship.**

The first column of Table 5 lists possible pre-market controls. The second column references the assumptions related to each control. The third column provides the CSF Subcategories potentially affected by the control, and the fourth column lists references to recommendations and requirements for the control in selected IoT guidance documents:

- BITAG: Broadband Internet Technical Advisory Group (BITAG), "Internet of Things (IoT) Security and Privacy Recommendations" [6]
- CSA1: Cloud Security Alliance (CSA) Mobile Working Group, "Security Guidance for Early Adopters of the Internet of Things (IoT)" [8]
- CSA2: CSA IoT Working Group, "Identity and Access Management for the Internet of Things" [7]
- ENISA: European Union Agency for Network and Information Security (ENISA), "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures" [9]
- OTA: Online Trust Alliance (OTA), "IoT Security & Privacy Trust Framework v2.5" [10]
- UKDDCMS: United Kingdom Government Department for Digital, Culture, Media & Sport (DCMS), "Secure by Design: Improving the cyber security of consumer Internet of Things" [11]

Table 5: Possible Pre-Market Controls for IoT Device Acquisitions

Control	Assumptions	CSF Subcategories	References to Selected IoT Guidance Documents
1. The IoT device should be uniquely identifiable both logically and physically.	1	ID.AM-1, 2 PR.AC-1 PR.DS-3 PR.MA-1, 2	• BITAG: 7.2, 7.6 • CSA1: 5.2.1.1, 5.3.1, 5.3.4 • CSA2: 11, 14 • ENISA: PS-10, TM-21 • UKDDCMS: 4
2. The sources of all the IoT device software, hardware, and services should be disclosed, confirmed, and certified according to secure supply chain policies throughout the device's lifecycle.	3 and 4	DE.CM-4 ID.SC-2, 3	• BITAG: 7.10 • CSA1: 5.2.2 • ENISA: OP-12, 14 • OTA: 9, 11
3. The IoT device should allow the administrator to access a current inventory on demand of its internal software and firmware, including versions and patch status.	3	DE.CM-8	• CSA1: 5.3, 5.5.3 • ENISA: TM-56 • UKDDCMS: 12
4. The IoT device should support a configurable, secure software and firmware update mechanism for the lifecycle of the device.	5 and 6	PR.IP-12 PR.MA-1, 2	• BITAG: 7.1 • ENISA: OP-02, 03, TM-18, 19 • OTA: 1, 6, 7, 8, 19 • UKDDCMS: 3
5. The IoT device administrator should be able to securely change configurations and prevent unauthorized changes to those configurations.	6	PR.IP-3	• CSA2: 02 • ENISA: TM-22 • OTA: 16
6. The IoT device should have a secure default configuration, and administrators should be able to restore the default configuration on demand.	6	PR.IP-1	• BITAG: 7.1 • ENISA: TM-09 • OTA: 13, 14, 26, 33 • UKDDCMS: 2, 11
7. The IoT device should enable enforcing the principle of least functionality through its design and/or configuration settings.	6	PR.PT-3	• BITAG: 7.2, 7.3 • CSA1: 5.3.2, 5.3.3 • ENISA: TM-08, 43-45, 50 • OTA: 12 • UKDDCMS: 6, 12

Control	Assumptions	CSF Subcategories	References to Selected IoT Guidance Documents
8. The IoT device should provide the ability to control local and remote logical access to itself and its interfaces.	8, 10, 11, 12, 13	PR.AC-3, 4 PR.PT-2	• BITAG: 7.2 • CSA1: 5.3.1, 5.3.3, 5.6 • CSA2: 01, 04, 13, 16 • ENISA: TM-21, 23, 27 • UKDDCMS: 4
9. The IoT device should be designed and built with physical security/access control in mind.	9 and 14	PR.PT-2	• BITAG: 7.3 • ENISA: TM-31 • OTA: 37
10. The IoT device should support the use of cryptography to secure stored and transmitted data, including privacy-enhancing cryptography that allows for the blinding of trusted transmission points.	15, 16, 17, and 22	PR.DS-1, 2	• BITAG: 7.2 • CSA1: 5.4.1, 5.5.3.2, 5.3.3 • CSA2: 08 • ENISA: OP-04, TM-04, 34, 36, 52 • OTA: 2, 3 • UKDDCMS: 4, 5, 8
11. The IoT device should support and use well-known and standardized protocols for data transmission.	17	PR.AC-5	• BITAG: 7.2 • CSA1: 5.4.1, 5.2.2, 5.3.1 • CSA2: 07, 08 • ENISA: OP-04, TM-24, 36, 37, 39, 52 • OTA: 2, 3, 34 • UKDDCMS: 5
12. The IoT device should support logging the pertinent details of security events and making them easily accessible to authorized personnel and systems.	18, 19, 20, and 21	DE.AE-3 DE.CM-1, 6, 7 PR.PT-1 RS.AN-1	• CSA1: 5.7 • CSA2: 09 • ENISA: OP-05, TM-55-57 • OTA: 4
13. The IoT device should be designed to enable reliable assumptions about PII processing such as including human user interfaces that enable individuals to interact with the device or supporting software that de-identifies PII.	23	N/A	• BITAG: 7.7 • ENISA: TM-10, 14 • OTA: 18, 20, 22, 26 • UKDDCMS: 11
14. The IoT device should be configurable to enable owners or operators to manage PII processing with sufficient granularity to meet defined privacy requirements.	25	N/A	• BITAG: 7.3 • ENISA: TM-12
15. The IoT device should support software that enables machine-readable data tags for PII processing permissions.	24	N/A	• ENISA: TM-10, 11 • OTA: 2, 12, 20, 25, 32 • UKDDCMS: 8

Acronyms and Abbreviations

API	Application Programming Interface
BITAG	Broadband Internet Technical Advisory Group
CSA	Cloud Security Alliance
CSF	Cybersecurity Framework
DCMS	Department for Digital, Culture, Media & Sport
ENISA	European Union Agency for Network and Information Security
IoT	Internet of Things
IP	Internet Protocol
IR	Internal Report
IT	Information Technology
LTE	Long-Term Evolution
NIST	National Institute of Standards and Technology
OT	Operational Technology
OTA	Online Trust Alliance
PII	Personally Identifiable Information
SLA	Service Level Agreement
SP	Special Publication
UI	User Interface
USB	Universal Serial Bus

References

[1] E. Simmon, NIST IR xxxx, "A Model for the Internet of Things (IoT)", to be published

[2] Joint Task Force, Draft NIST SP 800-37 Revision 2, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," May 2018, https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/draft

[3] S. Brooks, M. Garcia, N. Lefkovitz, S. Lightman, and E. Nadeau, NIST IR 8062, "An Introduction to Privacy Engineering and Risk Management in Federal Systems," January 2017, https://doi.org/10.6028/NIST.IR.8062

[4] NIST, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," April 16, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[5] Joint Task Force, Draft NIST SP 800-53 Revision 5, "Security and Privacy Controls for Information Systems and Organizations," August 2017, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft

[6] BITAG, "Internet of Things (IoT) Security and Privacy Recommendations," November 2016, https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

[7] CSA IoT Working Group, "Identity and Access Management for the Internet of Things," September 2015, https://cloudsecurityalliance.org/download/identity-and-access-management-for-the-iot/

[8] CSA Mobile Working Group, "Security Guidance for Early Adopters of the Internet of Things (IoT)," April 2015, https://cloudsecurityalliance.org/download/new-security-guidance-for-early-adopters-of-the-iot/

[9] ENISA, "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures," November 2017, https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[10] OTA, "IoT Security & Privacy Trust Framework v2.5," June 2017, https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf

[11] United Kingdom Government DCMS, "Secure by Design: Improving the cyber security of consumer Internet of Things," March 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf