Considerations for a Core IoT Cybersecurity Capabilities Baseline

Through this draft discussion paper, NIST aims to gather feedback to help identify core IoT cybersecurity capabilities that are most vital for Internet of Things (IoT) devices. This paper presents one possible approach to developing baselines[1], which includes our initial thoughts about what a core baseline of cybersecurity capabilities that are important for most IoT devices would look like. In this paper, "baseline" is used in the generic sense to refer to a set of foundational requirements or recommendations. These could be used by IoT device manufacturers to guide the cybersecurity capabilities they implement in their products, as well as be used as a starting point by communities of interest to develop baselines appropriate to their community.

NIST welcomes feedback from all stakeholders. We are seeking guidance on the direction of this work, our approach to identifying and assessing baseline candidates, and the core IoT device cybersecurity capabilities baseline candidates proposed in this paper. For those who cannot engage with NIST in person, we encourage sending feedback to IoTsecurity@nist.gov.

Background

In recognition of a critical cybersecurity gap, NIST released draft NIST Internal Report (NISTIR) 8228: *Considerations for Managing IoT Cybersecurity and Privacy Risks* in September 2018. Through related stakeholder engagement, comments received during the NISTIR 8228 public comment period, and, as described below, the *Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*, NIST identified another critical gap area in guidance on baselines for IoT device cybersecurity. In particular, there was interest in baselines focused on the pre-market cybersecurity capabilities[2] that could be built into the products, as opposed to the cybersecurity controls[3] that consumers could apply post-market.

In May 2018, the Departments of Commerce and Homeland Security published the *Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*. Known as the Botnet Report, this report was developed in response to the May 11, 2018, Executive Order (EO) 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure."[4] As explained in the Botnet Report, resilience against botnets will require a multi-pronged approach, with many of the report's recommended actions being mutually supportive by design. The report called for the federal government to clearly delineate priorities for

[1] The term "baseline" should not be confused with the low, moderate, and high control security baselines set forth in NIST Special Publication 800-53 to help federal agencies meet their obligations under the Federal Information Security Modernization Act (FISMA) and other federal policies.
[2] Capabilities are functions or features (which may be achieved through different controls) that devices need in order to be able to achieve one or more higher-level risk mitigation goal(s). This definition is from NISTIR 8228.
[3] Cybersecurity controls are the management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. This definition is from NISTIR 7298.
[4] Exec. Order No. 13800, 82 Fed. Reg. 22391, at 22394 (May 11, 2017): https://federalregister.gov/d/2017-10004

action, and a road map was later released to identify tasks and timelines for completion. Recognizing that there is no one-size-fits-all, each of these recommendations and associated actions and tasks works towards achieving the overall goal of a more secure internet ecosystem. The road map also helps to sequence actions and tasks to achieve maximum benefit. As explained in the road map, before assessment, labeling, or awareness initiatives for IoT devices can begin, there first needs to be the foundational task of describing a core cybersecurity baseline, which is a set of cybersecurity capabilities that are broadly applicable across many or all IoT devices.

The road map calls on NIST, in collaboration with stakeholders, to identify a core set of cybersecurity capabilities, which can also be used to support vertical- or sector-specific baselines as needed, such as the federal government or home consumers. An identified core set of these capabilities would encourage harmonization and indicate the minimum cybersecurity capabilities any IoT device should support.

A core baseline can serve as a foundation upon which more detailed and rigorous baselines for individual sectors and verticals can be developed. For example, a connected medical device would likely require more cybersecurity capabilities than an IoT light bulb.

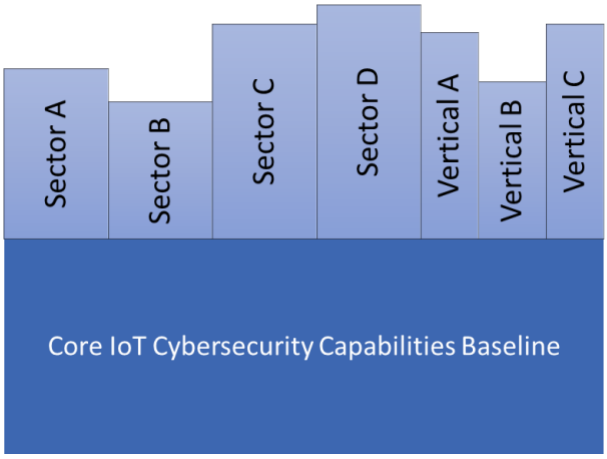

Figure 1: Visualization of how the core capabilities baseline discussed in this essay can be the foundation for baselines in varying sectors and verticals. Please note, sector refers to industry market sectors (e.g., energy, government, healthcare), while vertical refers to device categories or types (e.g., smart thermostat, e-reader, wearable health monitor).

Approach

NIST seeks to identify and propose a minimum set of cybersecurity *capabilities* (as opposed to controls) for IoT devices. These are capabilities all IoT devices should include that enable organizations and consumers to build more robust cybersecurity protections. This paper is informed, in part, by NISTIR 8228, which discusses IoT cybersecurity through the lens of device security and data security. The NISTIR notes that applying both traditional IT and IoT-specific cybersecurity measures require devices capable of performing certain primitive cybersecurity tasks (e.g., asset identification, secure updates, data encryption), suggesting the need for a core set of capabilities that covers these primitive tasks.

In Appendix A of NISTIR 8228, NIST developed such a list by identifying and analyzing common concepts in existing IoT cybersecurity guidance, frameworks, and standards from both domestic and international private and public sectors. Through this research, we found 15 capabilities frequently specified in existing guidance that targeted the risk mitigation areas identified in NISTIR 8228 Section 4 (access management, vulnerability management, etc.)

Through continued revision and based on public comments received, the phrasing of some capabilities was edited, and one capability for securely erasing a device's internal storage was added. This raised the list of capabilities in NISTIR 8228 Appendix A to 16 – specifically 12 being cybersecurity-focused, and 4 being privacy-focused.

While recognizing the importance of privacy considerations for IoT, this initial baseline will only feature capabilities that specifically address cybersecurity. A number of privacy efforts are currently underway that we believe are likely to inform needed device capabilities to support privacy.[5] Therefore, while the current work will consider and understand the privacy risks that security capabilities may introduce (as part of the baseline development), the privacy-focused capabilities from NISTIR 8228 Appendix A list were not considered. The remaining 12 edited cybersecurity capabilities serve as only a starting set of candidates for a core baseline that will be modified based on internal assessment and feedback from external stakeholders (Table 1).

Further analysis was done to identify the key considerations that could be used to identify candidates most qualified for inclusion in the core baseline. NIST is suggesting the following criteria to start the discussion for assessing core baseline candidates:

1. Utility: How critical is the capability towards improving the cybersecurity of IoT devices and data?
    a. When used alone, does the capability directly improve the cybersecurity?
    b. Do other cybersecurity capabilities rely on this capability to function?
    c. Which cybersecurity risk mitigation areas does the capability help achieve?
2. Verifiability: Can proper implementation of the capability be verified?
3. Feasibility: Are there roadblocks to implementing the capability that will make the device overly costly or complex, or less interoperable?
    a. Are the hardware, firmware, software, services, or protocols needed to implement the capability limited in availability or not industry accepted?

NIST suggests that items which have the most utility, are most readily verified, and are most feasible should be included in the core baseline.

[5] Additional information about the NIST Privacy Engineering Program and the NIST Privacy Framework: *An Enterprise Risk Management Tool* are available online.

Assessment of Initial Core Baseline Candidates

In Table 1, we present our assessment of the initial set of 12 IoT device cybersecurity baseline candidates using the criteria explained above. In addition to initial assessments of each candidate, the table also includes examples of potentially affected Cybersecurity Framework (CSF) subcategories and draft NIST Special Publication (SP) 800-53 controls, and existing IoT reference guidance from NISTIR 8228 Appendix A.

Capabilities 1-8 represent the initial proposed baseline of core cybersecurity capabilities that would apply to all or most IoT devices.[6] Capabilities in lines 9-12 may not be suitable for inclusion in the core baseline based on the assessment criteria considered, even though these were originally included in NISTIR 8228 Appendix A.

Table 1 is meant to provide context on our thinking about what is important for a core baseline, and our approach to assessing capabilities under consideration. The proposed baseline candidates will be updated based on stakeholder feedback. NIST is particularly interested in stakeholder input on the following questions:

1. Are these reasonable capabilities for a core baseline?
   a. Is the value to cybersecurity for each capability **apparent**?
   b. Should we **add** or **remove** any capabilities?
2. Are the capabilities **defined with enough specificity** to be useful to a manufacturer or other stakeholders?
3. Is this a reasonable approach to establish high-level objectives/principles/capabilities for devices and allow for communities of interest to identify the **appropriate standards** or detailed guidance on how best to **support those capabilities**?
4. Are the **criteria reasonable** for identifying baseline capabilities?
5. Would a **taxonomy** be helpful or needed to describe classes or types of devices to further parse or frame the baseline capabilities?

We do not intend these questions to limit thought or discussion about this work. All feedback will be considered when developing the next iteration of this baseline, which will become part of a broader NIST paper about core cybersecurity capabilities for IoT devices. Stakeholder feedback on the proposed criteria, assessments, and baseline candidates will ultimately help NIST to develop a baseline with the goal of producing a set of capabilities that not only effectively improves the cybersecurity of IoT devices, but also is practical for manufacturers to adopt. However, this core is only a foundation, and NIST anticipates that it will be built upon for the many sectors and verticals emerging in the IoT market.

[6] There may be a class of IoT devices that are limited by short lifespans or minimal capabilities. For these devices, some of the capabilities included may prove too restrictive and add little to no cybersecurity. Although we acknowledge the existence of such devices, this essay is intended to present the baseline for all other IoT devices.

Table 1: The 12 core IoT device cybersecurity capabilities baseline candidates considered so far. Assessment of each is based on the criteria explained above, and we also include a conclusion of why we think the candidate should or should not be included in the baseline. Finally, with each candidate, potentially affected Cybersecurity Framework (CSF) subcategories and draft NIST Special Publication (SP) 800-53 controls are reproduced from NISTIR 8228 Appendix A.

Baseline Candidate	Assessment Using Criteria	NIST CSF Subcategories	Draft NIST SP 800-53 Rev. 5 Controls	References to Selected IoT Guidance Documents
1. The IoT device can be identified both logically and physically.	The ability to monitor a network and identify rogue devices requires the ability to identify each device on the network. This can be verified by looking for logical and physical identifiers. Methods to create and assign/affix an identifier to a device during production are readily available, including standardized methods of generating identifiers. **This capability meets all three criteria and should be included in the core baseline.**	• ID.AM-1, 2 • PR.AC-1 • PR.DS-3 • PR.MA-1, 2	• CM-8 • IA-3 • PE-20	• BITAG[7]: 7.2, 7.6 • CSA1[8]: 5.2.1.1, 5.3.1, 5.3.4 • CSA2[9]: 11, 14 • CTIA[10]: 4.13 • ENISA[11]: PS-10, TM-21 • GSMA[12]: CLP11_5.2.1, CLP13_6.6.2, 6.8.1, 6.20.1, 8.11.1 • IIC[13]: 7.3, 8.5 • IoTSF[14]: 2.4.14.3-4, 2.4.8.1 • UKDDCMS[15]: 4
2. The IoT device's software and firmware can be updated using a secure, controlled, and configurable mechanism.	Software flaws are common and almost unavoidable, making the ability to update software and firmware necessary. Verifying the update processes' own cybersecurity may require deeper analysis than verifying update configurability. Providing an update mechanism and regular updates may increase the cost and complexity of devices and their development processes. **Though verification and implementation may be difficult in some contexts, the utility of this capability towards ongoing**	• PR.IP-12 • PR.MA-1, 2	• CM-3, 6 • SI-2	• BITAG: 7.1 • CSA1: 5.5.3.1 • CTIA: 3.5, 3.6, 4.5, 4.6, 5.5, 5.6 • ENISA: OP-02, 03, TM-06, 18, 19, 20 • GSMA: CLP11_5.3.3, CLP12_5.8.1, 5.9.1.3, 6.6.1 • IIC: 7.3, 10.5.3, 11.1, 11.2, 11.5 • IoTSF: 2.4.5, 2.4.6, 2.4.13.1

[7] Broadband Internet Technical Advisory Group (BITAG), "Internet of Things (IoT) Security and Privacy Recommendations," November 2016.
[8] Cloud Security Alliance (CSA) Mobile Working Group, "Security Guidance for Early Adopters of the Internet of Things (IoT)," April 2015.
[9] CSA IoT Working Group, "Identity and Access Management for the Internet of Things," September 2015.
[10] CTIA, "CTIA Cybersecurity Certification Test Plan for IoT Devices, Version 1.0," August 2018.
[11] European Union Agency for Network and Information Security (ENISA), "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures," November 2017.
[12] Groupe Spéciale Mobile Association (GSMA), "GSMA IoT Security Assessment," 2017.
[13] Industrial Internet Consortium (IIC), "Industrial Internet of Things Volume G4: Security Framework," 2016.
[14] IoT Security Foundation (IoTSF), "IoT Security Compliance Framework, Release 1.1," December 2017.
[15] United Kingdom Government Department for Digital, Culture, Media & Sport (DCMS), "Secure by Design: Improving the cyber security of consumer Internet of Things Report," March 2018.

Baseline Candidate	Assessment Using Criteria	NIST CSF Subcategories	Draft NIST SP 800-53 Rev. 5 Controls	References to Selected IoT Guidance Documents
	cybersecurity support indicates it should be included in the core baseline.			• OTA[16]: 1, 6, 7, 8, 9, 19 • UKDDCMS: 3
3. Authorized users can securely change the IoT device's configuration, including restoration to a secure "default." Unauthorized changes to the IoT device's configuration can be prevented.	Configurability allows users to adapt device functionality to better suit their needs. Shipment with secure and restorable default configurations can help protect against many blanket attacks. Configurability and restorability are verified by attempting to configure/restore the IoT device, but verification of the configuration processes' own cybersecurity may require deeper analysis. The ability to configure a device may add cost and complexity to the device and its development process. **Though verification and implementation may be difficult in some contexts, the utility of this capability towards allowing the tailoring of device capabilities (including those for cybersecurity) indicates it should be included in the core baseline.**	• PR.IP-1, 3	• CM-2, 6 • SC-42	• BITAG: 7.1 • CSA1: 5.3.3 • CSA2: 02 • CTIA: 4.7, 4.8, 4.12, 5.15 • ENISA: TM-06, 09, 22 • GSMA: CLP12_5.3.1.3, 5.6.2 • IIC: 7.6, 8.10, 11.1, 11.2, 11.5, 11.6 • IoTSF: 2.4.7.7, 2.4.8, 2.4.15 • OTA: 13, 14, 16, 26, 33 • UKDDCMS: 1, 11
4. Local and remote access to the IoT device and its interfaces can be controlled.	Controlling access is imperative for both ensuring confidentiality of data-at-rest on the device and controlling device behavior, which helps reduce the propensity and impact of attacks that use IoT devices against targets. Testing and verification of access control measures is possible, but may be difficult with diverse devices at scale. Greater access control may increase the complexity of a device or the system it resides in. **Though complexity of some devices and systems may increase to provide this capability and verification at scale may be difficult, its utility towards both device and data security indicates it should be in the core baseline.**	• PR.AC-3, 4 • PR.PT-2	• AC-2, 3, 4, 12, 14, 17 • CM-5 • IA-2, 3, 4, 5, 8, 9, 11 • MP-2 • SC-7	• BITAG: 7.2 • CSA1: 5.3.1, 5.3.3, 5.6 • CSA2: 01, 04, 13, 16 • CTIA: 3.2, 3.3, 3.4, 4.2, 4.3, 4.5, 4.7, 4.9, 4.10, 5.2, 5.5, 5.17 • ENISA: TM-09, 21, 23, 27, 29, 40 • GSMA: CLP12_5.6.1, 6.3.1.1, 7.1.1.2, CLP13_6.12.1, 7.10.1, 8.2.1.1 • IIC: 7.3, 8.6, 9.2.7, 11.7 • IoTSF: 2.4.4.5, 2.4.5, 2.4.6, 2.4.7, 2.4.8, 2.4.13, 2.4.15 • UKDDCMS: 4
5. The IoT device can use cryptography to secure its stored and transmitted data.	The ability to encrypt and decrypt data securely is fundamental to the overall security of data. Use of cryptography should be verifiable through data inspection. Many public cryptographic algorithms and modules are widely available, including those designed for resource-	• PR.DS-1, 2	• SC-8, 12, 13, 28, 40	• BITAG: 7.2 • CSA1: 5.3.1, 5.4.1, 5.5.3.2, 5.3.3, 5.7.3 • CSA2: 08

[16] Online Trust Alliance (OTA), "IoT Security & Privacy Trust Framework v2.5," June 2017.

Baseline Candidate	Assessment Using Criteria	NIST CSF Subcategories	Draft NIST SP 800-53 Rev. 5 Controls	References to Selected IoT Guidance Documents
	constrained devices. **This capability meets all three criteria and should be included in the core baseline.**			• CTIA: 4.8, 5.15 • ENISA: OP-04, TM-04, 24, 34, 36, 52 • GSMA: CLP12_5.1.5, 5.1.7.1, 5.2.2.1, 5.3.1.1, 6.2.1, 6.3.1.2, CLP13_6.1.1.6, 6.1.1.8, 6.4.1.1, 6.5.1.1, 6.11, 6.12.1.1, 7.6.1, 8.11.1 • IIC: 7.3, 7.4, 7.7, 8.8, 8.11, 9.1 • IoTSF: 2.4.5, 2.4.7, 2.4.8.8, 2.4.9, 2.4.12.2, 2.4.13.16 • OTA: 2, 3 • UKDDCMS: 4, 5, 8
6. The IoT device can use industry-accepted, standardized protocols for all layers of the device's transmissions.	These protocols can help avoid vulnerabilities in transmission due to faulty proprietary or esoteric communication methods. Use of specific protocols should be verifiable by inspection. In some instances, their use may be obscured within encrypted network communications and thus require external disclosure to verify. Though some transmission protocols can be resource-intensive, all IoT devices already send data over networks, so implementing specific, standardized protocols should be feasible in most contexts. **This capability meets all three criteria and should be included in the core baseline.**	• PR.AC-5 • PR.DS-2, 5	• AC-18 • SC-8	• BITAG: 7.2, 7.6 • CSA1: 5.4.1, 5.2.2, 5.3.1 • CSA2: 07, 08 • CTIA: 4.8, 5.14 • ENISA: OP-04, TM-24, 36, 37, 39, 52 • GSMA: CLP12_6.13.1.1, CLP13_6.3.1.2, 6.4.1.1 • IIC: 7.3, 7.4, 7.7, 9.1 • IoTSF: 2.4.5, 2.4.7, 2.4.9, 2.4.10 • OTA: 2, 3, 34 • UKDDCMS: 5
7. The IoT device can log the pertinent details of its cybersecurity events and make them accessible to authorized users and systems.	Logs provide the ability to audit events and reactions, and to monitor the cybersecurity and stability of a network and its devices, which is important for achieving and maintaining secure operation. Creation of and access to logs is verified by inspection, but assessing completeness and utility is partly subjective and less readily verified. A robust event detection and logging system may be resource-intensive and thus could increase the cost and complexity of devices and their development. **Though complexity of some devices may increase to provide this capability and verification of completeness may be**	• DE.AE-3 • DE.CM-1, 6, 7 • PR.PT-1 • RS.AN-1	• AU-2, 3, 6, 7, 8, 9, 12 • IR-4, 5 • SI-3, 4, 7	• CSA1: 5.5.4, 5.7 • CSA2: 09 • CTIA: 4.7, 4.12, 4.13, 5.7 • ENISA: OP-05, TM-55-57 • GSMA: CLP11_5.3.4, CLP12_5.7.1.2, 5.7.1.3, CLP13_6.13.1, 7.2.1, 9.1.1.2 • IIC: 7.3, 7.5, 10.1, 10.2, 10.3.2 • OTA: 4 • UKDDCMS: 2, 10

Baseline Candidate	Assessment Using Criteria	NIST CSF Subcategories	Draft NIST SP 800-53 Rev. 5 Controls	References to Selected IoT Guidance Documents
	difficult, its utility towards maintaining both device and data security suggests it should be in the core baseline.			
8. The IoT device can be reset by authorized users so all data-at-rest on the device is securely removed from all internal data storage.	Cybersecurity risk management over the lifecycle of a device requires preventing logical or physical access to data previously stored on the device when it is decommissioned. This should be verifiable through testing of the product. The complexity of providing a secure data reset/erasure capability may depend on the complexity of the underlying storage design and architecture. **This capability meets two of three criteria, but we argue that feasibility is only limited in complex data storage schemes. Thus, this capability should be included in the core baseline.**	• PR.IP-6	• MP-6	Because this is a new candidate, the reference mappings have not yet been documented.
9. Information confirming the sources of all of the IoT device's software, firmware, hardware, and services is disclosed and accessible.	*This is important for users looking to reduce risks through secure supply chain practices. Availability of information is easily verified, but confirmation of the information's completeness may be difficult. Information for component sources produced further up a supply chain may not be readily available or may be costly for a manufacturer to access and compile.* ***Though this capability may offer utility, it would be difficult to adequately verify and harder to implement, so it should not be in the core baseline.***	• DE.CM-4 • ID.SC-2, 3	• AC-20 • CM-8, 10 • IA-9 • SA-9, 12, 19 • SI-7	• BITAG: 7.10 • CSA1: 5.2.2 • CSA2: 14 • CTIA: 3.1.4 • ENISA: OP-14 • GSMA: CLP12_5.1.2.1, 7.1.1.1, CLP13_9.7.1 • IIC: 7.3, 7.5, 10.5.3 • OTA: 9, 11 • UKDDCMS: 7
10. An inventory of the IoT device's current internal software and firmware, including versions and patch status, is disclosed and accessible.	*This is useful for update management but not necessary in all update mechanisms. Availability of information is easily verified, but confirmation of the information's completeness may be difficult. Disclosing version and status for all device components may be difficult due to black box hardware and software used in a device.* ***This capability would offer limited utility, could prove difficult to adequately verify, and may be difficult to implement, so it should not be in the core baseline.***	• DE.CM-8	• CM-8, 10, 11 • RA-5	• CSA1: 5.2.2, 5.3, 5.5.3 • CSA2: 14 • CTIA: 3.5, 4.5, 5.5, 5.6 • ENISA: TM-56 • GSMA: CLP12_5.9.1.3, CLP13_6.1.1, 9.7.1.2 • IIC: 7.3, 7.5, 10.5.3 • IoTSF: 2.4.6.2 • OTA: 9 • UKDDCMS: 12

Baseline Candidate	Assessment Using Criteria	NIST CSF Subcategories	Draft NIST SP 800-53 Rev. 5 Controls	References to Selected IoT Guidance Documents
11. *The IoT device can enforce the principle of least functionality through its design and configuration.*	*Limiting functionality as a general design practice can improve device and data security by limiting the attack surface. Verifying design principles is difficult and requires organizational access. Designing for least functionality or extending a design to allow for functionality configuration may increase the cost and complexity of the device's development process.* ***Though this capability may offer utility, it would be very difficult to verify and might also be costly to implement, so it should not be in the core baseline.***	• PR.PT-3	• CM-7	• BITAG: 7.2, 7.3 • CSA1: 5.3.2, 5.3.3 • CSA2: 12, 13, 16 • CTIA: 5.17 • ENISA: TM-05, 08, 12, 27, 28, 43-45, 50 • GSMA: CLP12_7.1.1.2, CLP13_6.7.1, 6.12.1.6, 7.9.1 • IoTSF: 2.4.6, 2.4.7.18, 2.4.13 • OTA: 12 • UKDDCMS: 6, 12
12. *The IoT device is designed to allow physical access to it to be controlled.*	*Physical access control is important for continuously securing devices, but it can be controlled post-market in many ways and in a diverse set of contexts (e.g., placement of devices in inaccessible locations or within more secure enclosures). Physical resilience of a device takes time and expertise to verify. Hardening physical access to internal components should be within the means of manufacturers already executing a product design and development process, but design considerations (e.g., form factor) could make achieving it difficult.* ***This capability would offer limited pre-market utility, could prove difficult to adequately verify, and may be difficult to implement, so it should not be in the core baseline.***	• PR.PT-2	• MP-2, 7 • SA-18 • SC-41	• BITAG: 7.3 • CSA2: 11 • CTIA: 5.16 • ENISA: TM-31, 32, 33 • GSMA: CLP13_7.3.1, 8.2.1.2 • IIC: 7.3, 7.4, 8.3 • IoTSF: 2.4.4 • OTA: 37