Before the

National Institute of Standards and Technology

DEPARTMENT OF COMMERCE

Washington, D.C. 20230

In the Matter of	)	
	)	
Core Cybersecurity Feature Baseline for Securable IoT Devices	)	Draft NISTIR 8259

COMMENTS OF THE OPEN CONNECTIVITY FOUNDATION

I. INTRODUCTION AND SUMMARY

The Open Connectivity Foundation (OCF) is seeking to provide *secure* interoperability for the Internet of Things (IoT) ecosystem through an industry-led, open and collaborative process. To achieve secure interoperability and drive adoption, OCF has delivered and published an interface specification, a certification regime, and an open source reference implementation ("IoTivity"). To further enhance credibility and adoption, OCF has successfully worked with ISO/IEC to have the OCF specification adopted as ISO/IEC standards.[1]

- OCF Interface Specification: OCF leverages existing and proven standards and technology to enable secure interoperability directly between IoT devices communicating locally as well as between IoT devices and the cloud, regardless of the manufacture, form factor, operating system, chipset, or physical transport.
- OCF Certification: OCF certification ensures conformance to the specification and provides consumers with confidence that OCF-certified products will seamlessly and securely work

[1] *E.g.*, ISO/IEC 30118-1:2018, Information technology — Open Connectivity Foundation (OCF) Specification — Part 1: Core specification, https://www.iso.org/standard/53238.html; ISO/IEC 30118-2:2018, Information technology — Open Connectivity Foundation (OCF) Specification — Part 2: Security specification, https://www.iso.org/standard/74239.html.

together, irrespective of manufacturer. To obtain OCF certification, IoT providers must submit their products and pass the comprehensive testing suite executed by an OCF approved, third-party laboratory.

- IoTivity: OCF sponsors a Linux Foundation Collaborative Project, entitled "IoTivity", that has developed and continues to maintain open source software that provides a reference implementation of the OCF specification, including an implementation framework for OCF's security controls.[2] The goal of IoTivity is to accelerate OCF adoption by lowering the cost and required technical resources to implement the specification.

OCF membership is broad-based with over 450 member organizations representing the full spectrum of the IoT ecosystem, from chip makers to consumer electronics manufacturers, including leading companies in silicon (e.g., Intel, Qualcomm), software (e.g., Microsoft), platform and finished-goods (e.g., Cisco, Samsung, LG), and network operators (e.g., CableLabs, Comcast).[3]

OCF has and continues to remain focused on cybersecurity. This is evident in the structure of the organization, the structure of the specification, and in the conformance testing. OCF has a dedicated "Security Work Group" that defines the security framework for each technology and solution defined by OCF.[4] Through this structure, security has been incorporated by design into every aspect of the OCF specification. Within the OCF specification, there is a dedicated "OCF Security Specification" that defines security objectives, philosophy, resources and mechanisms, including includes device identity, authentication, provisioning, establishing network credentials, authorization, and access control within the OCF resource-oriented architecture. The OCF Security Specification also address confidentiality, message integrity, resource persistence protections, and

---

[2] IoTivity, Linux Foundation, https://iotivity.org/.
[3] Membership List, Open Connectivity Foundation, https://openconnectivity.org/foundation/membership-list.
[4] Organizational Structure, Open Connectivity Foundation, https://openconnectivity.org/foundation/organizational-structure.

securing exchanges between local and remote devices or hosts.[5] Lastly, the OCF Certification Program includes conformance testing to ensure devices are built to the specification. Of the required conformance tests, over half relate to security.[6]

OCF's commitment to security is further demonstrated by its work and contributions to the broader IoT industry – most notably, the recent "C2 Consensus on IoT Device Security Baseline Capabilities."[7] This past March, the Consumer Technology Association (CTA) and the Council for Securing the Digital Economy (CSDE) hosted a workshop that brought together a broad swath of industry to begin developing a consensus on baseline IoT security capabilities.[8] The workshop kicked off a multi-month process to develop the recently released consensus. Throughout that process, OCF was actively engaged to help drive robust IoT device security and design practices. Not only did OCF push for a robust C2 Consensus, but OCF has also implemented nearly all of the identified baseline capabilities and more, as detailed in the attached Appendix.

OCF generally supports NIST's work in IoT security and specifically its development of a core cybersecurity feature baseline for IoT. More broadly, OCF urges NIST to work with global governments to help ensure harmonization of IoT security policy to accelerate the promised benefits of IoT. OCF not only agrees with the specific baseline features identified by NIST, but more importantly, OCF has already implemented nearly all of the identified features in its specification and in the associated open source implementation. OCF is currently working through how to implement

---

[5] OCF Specifications 2.0.5, Specifications, Open Connectivity Foundation, https://openconnectivity.org/developer/specifications.

[6] Open Connectivity Foundation Certification Test Requirements, Version 1902.0.1, Open Connectivity Foundation (June 5, 2019), https://workspace.openconnectivity.org/kws/test_tools/Certification_Test_Requirements_v1902.0.1.pdf [member login required].

[7] The C2 Consensus on IoT Device Security Baseline Capabilities, Council for Securing the Digital Economy (Sept. 2019), https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf.

[8] Landmark IoT Security Summit Gathers Industry Cybersecurity Experts and Leaders to Build Cross-Sector Guidelines for Securing Connected Devices, BusinessWire (Mar. 21, 2019), https://www.businesswire.com/news/home/20190321005773/en/Landmark-IoT-Security-Summit-Gathers-Industry-Cybersecurity.

"cybersecurity event logging" and believes industry would benefit from further guidance from NIST in this area. More generally, OCF supports NIST's flexible approach to implementing the identified cybersecurity features, the recommendation that IoT manufactures use established IoT platforms, and the need to clearly communicate cybersecurity information to customers. However, OCF suggests NIST separate the core baseline of cybersecurity features (Section 4) from the business practice guidance (Sections 3, 5, 6, and 7) and place this latter guidance in its own separate, standalone document.

II. DISCUSSION

a. NIST's work on IoT security is needed and necessary to drive increased security in all IoT devices.

OCF strongly supports NIST's work and leadership on IoT security and specifically, its initiative to create a core cybersecurity feature baseline for IoT devices through the development of Draft NISTIR 8259. There is no shortage of broad recommendations, white papers, and proposed best practices on IoT security; however, as the expert federal agency on cybersecurity, NIST has a unique and authoritative role to help bring clarity and certainty to the market in the US and abroad. In order to realize the consumer benefits and unique innovation promised by IoT devices and applications, everyone in the ecosystem (from entrepreneurs and small startups to mature global companies and their customers) needs clear, straightforward leadership and guidance that will decrease investment risks and build trust and confidence between parties, both in the United States and globally. Increased global harmonization of IoT security standards, baselines, and best practices will help facilitate and accelerate the promised benefits of IoT – to enrich our lives and drive significant productivity gains in the broader economy.

b. OCF urges NIST to work closely with its peers globally to drive harmonization of IoT security policy to help accelerate the promise of IoT.

OCF encourages NIST to continue building consensus and working towards global harmonization alongside its international counterparts both in the European Union (EU) and more broadly. Robust and internationally harmonized IoT security policy is critical to mitigating cybersecurity risks in the US and globally and to enabling the necessary economies of scale to

accelerate adoption and the promised benefits of IoT. Given the global nature of the security challenges posed by insecure IoT as well as the global market for IoT devices, it has become clear that no single government or industry actor will be able to alone fully address the challenge of insecure IoT, and cooperation and consensus across geographies and industries are needed to more fully address this challenge.

Although there is broad recognition of the risks associated with insecure IoT among policymakers globally, governments are approaching how to address these risks differently, particularly in how they view the role of government visa vie the role of industry and market forces. Not surprisingly, U.S. policymakers currently see industry-led initiatives and a close partnership with industry as the preferred approach, while the EU is approaching these challenges through more centralized, government-led efforts. The EU has put in place high-level security requirements applicable to IoT and is expected to continue to develop more specific requirements through government-led certification regimes.[9] OCF urges NIST to continue to build a collaborative relationship with the EU and other governments globally to ensure IoT security guidance, norms, and requirements emerge that are compatible and can allow a single implementation by a manufacture, enabling economies of scale that can help lower costs for US consumers. OCF believes viable approaches to insecure IoT must address the global nature of the security risks and work towards harmonization across geographies.

c. OCF not only supports the NIST-identified core IoT cybersecurity baseline features, it delivers those features and more.

OCF agrees that the core cybersecurity features identified in Draft NISTIR 8259 are necessary as a baseline for manufacturers to consider incorporating in their IoT devices. The

---

[9] *See, e.g.*, Baseline Security Recommendations for IoT, ENISA (Nov. 20, 2017), https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot; European Commission, *The EU Cybersecurity Act* (June 26, 2019), https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act.

current, publicly available OCF specification implements nearly all of the identified features in a robust and sound manner.[10] But that is just the start, through OCF's publicly available, open source implementation, IoTivity, OCF enables a manufacturer to easily incorporate these core features – the code has already been written and is available free of charge.[11] Moreover, through OCF's certification testing program, manufacturers can verifiably demonstrate to consumers that these features have been incorporated.[12] Table 1, below, provides the mapping of the OCF specification to the core cybersecurity features identified in Draft NISTIR 8259.

The core features identified in Draft NISTIR 8259 are a necessary foundation, but OCF's cybersecurity controls do not end there. OCF not only provides nearly all of the NIST-identified core baseline security features, but also provides nearly all of the C2 Consensus cybersecurity capabilities, even when looking beyond the "Baseline" capabilities to include the "Phase In Over Time" and "Additional IoT Device Security Capabilities and Practices," as detailed in the Appendix to these comments.[13]

---

[10] The one outlier is "cybersecurity event logging" – OCF is considering if and how to implement within the OCF specification to further support manufacturers in increasing security of IoT devices. But, to be clear, nothing in the OCF specification prevents a manufacturer from implementing cybersecurity event logging into the manufacturer's devices alongside the OCF implementation.
[11] Downloads, IotTivity, Linux Foundation Collaborative Projects (2019), https://iotivity.org/downloads.
[12] *See* OCF Certification, Open Connectivity Foundation, https://openconnectivity.org/certification/ocf-certification.
[13] The C2 Consensus on IoT Device Security Baseline Capabilities, *supra note* 7, at 10-26.

Table 1. Mapping NIST Capabilities to OCF Specification References.

NIST Core Feature	Key Feature Elements	OCF Reference
Device Identification: The IoT device can be uniquely identified logically and physically.	1. A unique logical identifier 2. A unique physical identifier on it at an external or internal location authorized entities can access	**[OCF Security Specification ISO/IEC 30118-2:2018] Clause 7.1.1.** The unique identifier for the device is either sent in the certificate the device sends when establishing communication on the network, or bound to a pre-shared key. **[OCF Security Specification ISO/IEC 30118-2] Clause 14.8.3** OCF recommends the use of a Public Key Infrastructure (PKI) for strong device identity and cryptographic capabilities through a certificate policy governing the operations and requirements for participating PKI participants and Certification Authorities (CAs).
Device Configuration: The IoT device's software and firmware configuration can be changed, and such changes can be performed by authorized entities only.	1. The ability to change the device's software and firmware configuration settings 2. The ability to restrict configuration changes to authorized entities only 3. The ability for authorized entities to restore the device to a secure default configuration defined by an authorized entity	**[OCF Security Specification ISO/IEC 30118-2:2018] Clauses: 5,6,7:** Prior to operational state, device must be onboarded and configured with either symmetric or asymmetric credentials based on certificates or shared keys. Once operational, devices implement role-based and/or subject based access control for each resource they present to the network. **[OCF Security Specification ISO/IEC 30118-2:2018] Clause 12:** Access control is enforced over all resources. **[OCF Security Specification ISO/IEC 30118-2:2018] Clause 13.3.1:** Stored Credentials used to authenticate server to clients. **[OCF Security Specification ISO/IEC 30118-2:2018] Clause 8.2:** Describes the resources and properties that are restored to manufacturer settings.

NIST Core Feature	Key Feature Elements	OCF Reference
Data Protection: The IoT device can protect the data it stores and transmits from unauthorized access and modification.	1. The ability to use accepted cryptographic algorithms (e.g., encryption with authentication, cryptographic hashes, digital signature validation) to prevent the confidentiality and integrity of the device's stored and transmitted data from being compromised 2. The ability for authorized entities to configure the cryptography use itself when applicable, such as choosing a key length 3. The ability for authorized entities to render all data on the device inaccessible by all entities, whether previously authorized or not (e.g., through a wipe of internal storage, destruction of cryptographic keys for encrypted data)	**[OCF Security Specification ISO/IEC 30118-2:2018] Clause 11.2.1:** Devices must support TLS/DTLS version 1.2 or greater for all unicast sessions. **[OCF Security Specification ISO/IEC 30118-2:2018] Clause 11.3:** Cipher Suites: All heavily reviewed and IETF approved or greater. **[OCF Security Specification ISO/IEC 30118-2:2018] Clause 14.2.2:** Secure storage for credentials is strongly recommended. **[OCF Vendor Attestation Document]:** Certification applicant has taken appropriate measures to protect Sensitive Data as defined in OCF Security Specification ISO/IEC 30118-2:2018 Clause 14.2.2 **[OCF Security Specification ISO/IEC 30118-2:2018] Clause 8.2:** Describes the Resources and properties that are restored to manufacturer settings during device reset.
Logical Access to Interferences: The IoT device can limit logical access to its local and network interfaces to authorized entities only.	1. The ability to logically or physically disable any local and network interfaces that are not necessary for the core functionality of the device. 2. The ability to logically restrict access to each network interface (e.g., device authentication, user authentication) 3. The ability to enable, disable, and adjust thresholds for any ability the device might have to lock or disable an account or to delay additional authentication attempts after too many failed authentication attempts.	**[OCF Security Specification ISO/IEC 30118-2:2018] Clause 12:** Describes access control and policy management for both local and network resources. **[OCF Security Specification ISO/IEC 30118-2:2018] Clause 5 Figure 3:** Shows security enforcement points.
Software and Firmware Update: The IoT device's software and firmware can be updated by authorized entities only using a secure and configurable mechanism.	1. The ability to update all the device's software and firmware through remote (e.g., network download) and/or local means (e.g., removable media) 2. The ability to confirm the validity of any update before installing it 3. The ability to restrict updating actions to authorized entities only 4. The ability to enable or disable updating 5. The ability to set remote update mechanisms to be either automatically or manually initiated for update downloads and installations 6. The ability to enable or disable notification when an update is available and specify who or what is to be notified	**[OCF Vendor Attestation Document]:** Certification Applicant agrees to respond to, address, and patch software vulnerabilities as prescribed by the OCF Security Incident Response Plan. **[OCF Security Specification ISO/IEC 30118-2:2018] Clause 14.5.3:** Process where device validates the software version against a trusted source. **[OCF Security Specification ISO/IEC 30118-2:2018] Clause 14.5.4:** A client with the correct authorization can initiate a software update process. **[OCF] Updatable Certified Product List:** Website - https://openconnectivity.org/certified-products. Manufacturers should notify OCF that device is End of Life (EoL).

NIST Core Feature	Key Feature Elements	OCF Reference
Cybersecurity Event Logging: The IoT device can log cybersecurity events and make the logs accessible to authorized entities only.	1. The ability to log cybersecurity events across the device's software and firmware 2. The ability to record sufficient details for each event to facilitate an authorized entity examining the log and determining what happened 3. The ability to restrict access to the logs so only authorized entities can view them 4. The ability to prevent any entities (authorized or unauthorized) from editing the logs 5. The ability to make the logs available to a logging service on another device, such as a log server	Cybersecurity Event Logging is an important area of future work for OCF.

d. OCF urges that NIST provide further guidance on the implementation of Cybersecurity Event Logging in IoT.

OCF requests that NIST consider developing IoT-specific guidance on the implementation of cybersecurity event logging. Such guidance would likely be beyond the scope of the current NISTIR 8259 and would likely warrant its own standalone publication. Specifically, manufacturers would benefit from an articulation of guideposts and other considerations in helping determine what events to log and other practical guidance on developing, implementing, and maintaining effective log management practices for IoT devices. While NIST has previously provided specific similar guidance on *computer* security log management,[14] IoT devices present unique challenges both in terms of the cyber-physical nature of the devices and the constrained nature of the devices (e.g., battery life, limited processing and storage) as well as the potential that log data may constitute personal data. Unlike the other identified cybersecurity features where implementations and tradeoffs in an IoT context are more widely understood, "cybersecurity event logging" in IoT is quite nascent and industry could further benefit from NIST's leadership and guidance in implementing this feature.

[14] Karen Kent & Murugiah Souppaya, *Guide to Computer Security Log Management*, NIST SP 800-92 (Sept. 2006), https://csrc.nist.gov/publications/detail/sp/800-92/final.

e. NIST correctly recognizes the necessity of a flexible approach to implementing the core cybersecurity features.

OCF commends NIST for clearly recognizing the need for flexibility in implementing the identified core baseline of cybersecurity features. Draft NISTIR 8259 appropriately includes recognition that "IoT device design processes may determine that certain cybersecurity features can be omitted from IoT devices because equivalent protection will be inherited from elsewhere."[15] Given the nascent state of IoT devices and wide breadth of possible and innovative applications possible, OCF supports the need for flexibility in implementing the core features to allow manufactures to adapt to specific use-cases and deployment contexts. For example, as Draft NISTIR 8259 recognizes, in some cases the IoT device itself has limited capabilities and cannot securely conduct all cybersecurity processes itself (e.g., cybersecurity event logging).[16] In such cases, the flexibility to abstract those functions to other devices in the network (e.g., a smart hub) is critical (e.g., potentially using off-device feature inheritance for event logging of constrained devices).

f. IoT manufacturers should generally use established IoT platforms to minimize cybersecurity risks.

OCF agrees wholeheartedly that using well-vetted and well-established IoT platforms increases the likelihood of delivering a more secure device, avoiding the risks of developing cybersecurity features from "scratch."[17] OCF provides one such well-vetted and well-established IoT platform.

---

[15] Michael Fagan, Katerina Megas, Karen Scarfone, & Matthew Smith, Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers, NISTIR 8259 (Draft) (Jul. 2019), https://csrc.nist.gov/publications/detail/nistir/8259/draft.

[16] *Id*.

[17] "Manufacturers may want to consider using an established IoT platform instead of acquiring and integrating hardware, firmware, and supporting software components (e.g., operating system). . . . Manufacturers can choose an adequately resourced IoT platform instead of designing hardware, installing and configuring an operating system or firmware, creating new cloud-based services, writing IoT device applications and mobile apps from scratch, and performing other tasks that are error-prone and generally *more likely to introduce new vulnerabilities into the IoT device compared to adopting an established platform*." *Id*. at 14-15 (emphasis added).

The OCF specification has been developed using an open, collaborative, consensus-based approach with over 450 organizations involved and leverages existing and proven standards and technology in the development of the platform. This is particularly true in the area of cybersecurity. For instance, all cipher suites are recognized IETF RFCs and most are IANA supported ciphers. Moreover, OCF only uses NIST-approved algorithms for all cryptographic operations.

OCF also uniquely provides an open source implementation of the platform.[18] Having a broad base of developers examining the open source software helps further reduce the risk of vulnerabilities, providing a further layer of vetting to help increase the confidence in the platform. Through its use of proven standards and technology along with the open source implementation enables OCF to deliver a well-vetted and well-established IoT platform to drive increased IoT security.

g. Clearly communicating cybersecurity information is critical in helping drive increased IoT security.

OCF agrees with and supports NIST's emphasis on transparency and providing clear communications on cybersecurity information to customers. Through an open, publicly available specification, OCF details exactly how it has implemented the core baseline features identified by NIST.[19] More fundamentally, OCF's certification testing program and associated certification mark provide consumers with confidence that the security features included in the specification are actually incorporated in the device. OCF certification requires conformity testing by OCF-approved third-party labs conducting a test suite developed by OCF. Through IoTivity – the OCF open source implementation, OCF provides further transparency including a list of all software dependencies, enabling a manufacture seeking to incorporate the IoTivity software to have a sound understanding of potential risks. OCF agrees with NIST that the form

[18] Downloads, IotTivity, Linux Foundation Collaborative Projects (2019), https://iotivity.org/downloads.
[19] *See supra* Table 1.

and detail of communications with customers will vary dramatically (e.g., from a certification mark to a full list of software dependencies) based on the customer targeted and their needs.[20]

h. NIST should consider publishing the core baseline of cybersecurity features (Section 4) and the business practice guidance (Sections 3, 5, 6, and 7) in separate documents.

As discussed above, OCF is generally in support of the substance of both the core baseline of cybersecurity features (Section 4) as well as the business practice guidance (Sections 3, 5, 6, and 7). However, a baseline set of cybersecurity features is materially different in purpose and scope from more generalized guidance on business practices. Having these two disparate substantive areas in the same document creates risk that they might be treated similarly by legislative bodies and other government agencies (particularly regulatory) as they continue to engage on the issue of IoT security. This risk is particularly acute as this work is considered outside the US.

III. CONCLUSION

OCF generally agrees with and supports NIST's work in IoT security and specifically its development of a core cybersecurity feature baseline for IoT. NIST should seek to work internationally to help harmonize IoT security policy to address both the risks posed by insecure IoT and to accelerate access to the promised benefits of IoT. In addition to agreeing with baseline features identified by NIST, OCF has already delivered nearly all of the identified features in its specification and in the associated OCF open source implementation. OCF is currently working through how to implement "cybersecurity event logging" and NIST should consider developing further guidance in this area. More generally, OCF supports NIST's flexible approach to implementing the identified cybersecurity features, the recommendation that IoT manufactures use established IoT platforms, and the need to clearly communicate cybersecurity information to

[20] Michael Fagan, Katerina Megas, Karen Scarfone, & Matthew Smith, Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers, NISTIR 8259 (Draft) (Jul. 2019), https://csrc.nist.gov/publications/detail/nistir/8259/draft.

customers. However, NIST should seperate the core baseline of cybersecurity features (Section 4) from the business practice guidance (Sections 3, 5, 6, and 7) and place this latter guidance in a separate document.

Should NIST have any questions in relation to these comments, please contact Mark A. Walker, Chair, OCF Technology Policy Work Group (m.walker@cablelabs.com), or by telephone at (303) 661-3466.

Respectfully Submitted,

/s/ **Mark A. Walker**

Mark A. Walker
Chair, Technology Policy Work Group, OCF
Director, Technology Policy, CableLabs

OCF
3855 SW 153rd Drive,
Beaverton, Oregon 97003
503-619-0673
www.openconnectivity.org

September 30, 2019

APPENDIX

Mapping of OCF Specification to the C2 Consensus

OCF provides the following mapping of its specification to the IoT security capabilities set forth in the C2 Consensus.[21] OCF continues to revise and expand its specification and associated conformance testing and certification program. To ensure access to the most accurate and up-to-date information on the OCF specification and testing and certification program, please visit https://openconnectivity.org.

C2 Consensus Category	C2 Consensus Sub-Category	OCF Specification
Secure Device Capabilities - Baseline	Device Identifiers	**[OCF Security Specification ISO/IEC 30118-2:2018] Clause 7.1.1.** The unique identifier for the device is either sent in the certificate the device sends when establishing communication on the network, or bound to a pre-shared key.
Secure Device Capabilities - Baseline	Secured Access	**[OCF Security Specification ISO/IEC 30118-2:2018] Clauses: 5,6,7:** Prior to operational state, device must be onboarded and configured with either symmetric or asymmetric credentials based on certificates or shared keys Once operational devices implement role-based and/or subject based access control for each resource they present to the network. **[OCF Security Specification ISO/IEC 30118-2:2018] Clause 12:** Access control is enforced over all Resources. **[OCF Security Specification ISO/IEC 30118-2:2018] Clause 13.3.1:** Stored Credentials used to authenticate server to clients. Note: OCF does not specify physical access controls.
Secure Device Capabilities - Baseline	Data in Transit Is Protected	**[OCF Security Specification ISO/IEC 30118-2:2018] Clause 11.2.1:** Devices must support TLS/DTLS version 1.2 or greater for all unicast sessions.
Secure Device Capabilities - Baseline	Data at Rest Is Protected	**[OCF Security Specification ISO/IEC 30118-2:2018] Clause 14.2.2:** Secure storage for credentials is strongly recommended. **[OCF Vendor Attestation Document]:** Certification applicant has taken appropriate measures to protect Sensitive Data as defined in OCF Security Specification ISO/IEC 30118-2:2018 Clause 14.2.2
Secure Device Capabilities - Baseline	Industry Accepted Protocols are Used for Communications	**[OCF Security Specification ISO/IEC 30118-2:2018] Clause 5 Figure 3:** Shows transport, session and application layer standards. **[OCF Security Specification ISO/IEC 30118-2:2018] Clause 11.2.1:** Devices must support CoAP, and CoAP over DTLS. **[OCF Security Specification ISO/IEC 30118-2:2018] Clause 11.3:** Cipher Suites: All heavily reviewed and IETF approved or greater.
Secure Device Capabilities - Baseline	Data Validation	**[OCF Core Technology Specification ISO/IEC 30118-1:2018].** Data model enforcement of encoding, type and length. Data model enforcement occurs on data inbound and outbound to the system. **Certification includes schema validation.**
Secure Device Capabilities - Baseline	Event Logging	Future work for OCF.

[21] The C2 Consensus on IoT Device Security Baseline Capabilities, *supra note* 7, at 44 ("Annex I: Mapping to Open Connectivity Foundation Specifications").

C2 Consensus Category	C2 Consensus Sub-Category	OCF Specification
Secure Device Capabilities - Baseline	Cryptography	**[OCF Security Specification ISO/IEC 30118-2:2018] Clause 11.3.1:** This clause lists the cipher suites allowed during ownership transfer and normal operation. All cipher suites are recognized IETF RFCs and most are IANA supported ciphers. Strong, proven, updateable cryptography using open, peer-reviewed methods and algorithms. NIST approved algorithms for all cryptographic operations.
Secure Device Capabilities - Baseline	Patchability	**[OCF Vendor Attestation Document]:** Certification Applicant agrees to respond to, address, and patch software vulnerabilities as prescribed by the OCF Security Incident Response Plan. **[OCF Security Specification ISO/IEC 30118-2:2018] Clause 14.5.3:** Process where device validates the software version against a trusted source. **[OCF Security Specification ISO/IEC 30118-2:2018] Clause 14.5.4:** A client with the correct authorization can initiate a software update process.
Secure Device Capabilities - Baseline	Re-provisioning	**[OCF Security Specification ISO/IEC 30118-2:2018] Clause 8.2** Defines how resources on the device are returned to the manufacturer's default values.
Product Lifecycle Management – Baseline	Vulnerability Submission and Handling Process	**[OCF] Security Working Group Incident Response Plan:** document addresses reporting (web page dedicated to reporting of issues), mitigation, timeframes, communication, emergency/critical fixes, and software deployment.
Product Lifecycle Management – Baseline	EoL/EoS Updates and Disclosure	**[OCF] Updatable Certified Product List:** Website. https://openconnectivity.org/certified-products manufacturers should notify OCF that device is EoL.
Produce Lifecycle Management - Baseline	Device Intent Documentation	**[OCF Security Specification ISO/IEC 30118-2:2018] Clause 9.4.2.2.3 End Entity Certificate Profile:** The MUD file pointed to by the URI included in the X.509 certificate includes the following properties referenced in RFC 8520: **[RFC 8520] Section 3.7 systeminfo (https://tools.ietf.org/html/rfc8520#section-3.7):** This is a textual UTF-8 description of the Thing to be connected. The intent is for administrators to be able to see a brief displayable description of the Thing. It SHOULD NOT exceed 60 characters worth of display space. **[RFC 8520] Section 4.3 documentation (https://tools.ietf.org/html/rfc8520#section-4.3):** This URI consists of a URL that points to documentation relating to the device and the MUD file.
Secure Capabilities - Phase in Over Time	Device Intent Signaling	**[OCF Security Specification ISO/IEC 30118-2:2018] Clause 9.4.2.2.3 End Entity Certificate Profile:** This section details the manner in which devices can signal intent and capabilities beyond those currently in use for security profiles. MUD URI's can be encoded here, as can attestations about meeting differing hardening requirements, certificate trust chains, and more.
Secure Capabilities - Phase in Over Time	Device Network Onboarding	**[OCF Security Specification ISO/IEC 30118-2:2018] Clause 3.1.31 Device Configuration Resource (DCR):** Includes the WiFi Easy Setup Resources, and the other transport-level onboarding (e.g. Bluetooth) are defined in other specification documents for OCF. **[OCF Security Specification ISO/IEC 30118-2:2018] Clause 5.3 Onboarding Overview:** For non-transport onboarding, the process is specified in great detail as far as establishment of trust, authentication, verification, authorization, local credential issuance, etc.
Additional IoT Device Security Capabilities and Practices	Secure Development Lifecycle	**[OCF Security Specification ISO/IEC 30118-2:2018] Clause 14.2.2.4: Additional Security Guidelines and Best Practices**: address Software and Secure Development Lifecycle, but OCF is not an application level specification, rather it is a Session-level specification so there will always be additional software added to the foundation OCF provides.

C2 Consensus Category	C2 Consensus Sub-Category	OCF Specification
Additional IoT Device Security Capabilities and Practices	Hardware Rooted Security	**[OCF Security Specification ISO/IEC 30118-2:2018] Clause 14.8.3.4: Black Security Profile:** requires the manufacturer to install a certificate which chains to the OCF root certificate (which is in each onboarding tool's trust store) to validate the hardware has been OCF Certified by an authorized test lab, that it chains to that manufacturer's intermediate root and that it shares a trust relationship bound to the hardware and secure credential store of the device. **[OCF Security Specification ISO/IEC 30118-2:2018] Clause 14.2.2.2:** Hardware Secure storage is recommended for symmetric and asymmetric keys, access credentials and personal private data. **[OCF Security Specification ISO/IEC 30118-2:2018] Clause 14.2.7:** Defines levels of Hardware Tamper Protection for cryptographic module.
Additional IoT Device Security Capabilities and Practices	Time Distribution	**[OCF Security Specification ISO/IEC 30118-2:2018] Clause 14.2.5:** Secure time source can be external as long as it is signed by a trusted source and the signature validation in the local device is a trusted process (e.g. backed by secure boot).
Additional IoT Device Security Capabilities and Practices	System Resiliency	**[OCF]:** Certification requires that all devices maintain proximal control in the case of a wide area network outage.
Additional IoT Device Security Capabilities and Practices	Secure Toolchains	**[OCF Security Specification ISO/IEC 30118-2:2018] Clause** 14.2.2.4-13**: Security Hardening Guidelines/ Execution Environment Security**: It is recommended that at least one static and dynamic analysis tool be applied to any proposed major production release of the software before its release, and any vulnerabilities resolved.
Additional IoT Device Security Capabilities and Practices	Software Transparency and Bill of Materials	IoTivity is an open source implementation for OCF and lists all software dependencies. https://iotivity.org/
Additional IoT Device Security Capabilities and Practices	Least Functionality	**[OCF Security Specification ISO/IEC 30118-2:2018] Clause 12: Access Control:** Employs a deny-all, permit-by-exception policy to allow access to Resources (data and actuators) for Read/Write/Create/Delete/Notify. Access control can be updated dynamically at the location of deployment to limit access (to a role, Device, or implementation).
Additional IoT Device Security Capabilities and Practices	Physical Access Control	**[OCF Security Specification ISO/IEC 30118-2:2018] Clause 14.2.7:** Defines levels of Hardware Tamper Protection for cryptographic module. **[OCF Security Specification ISO/IEC 30118-2:2018] Clause** 14.2.2.4: Additional Security Guidelines and Best Practice
Additional IoT Device Security Capabilities and Practices	Best Current Practices	**[OCF Security Specification ISO/IEC 30118-2:2018] Clause 14.2.2.4: Additional Security Guidelines and Best Practices:** Discuss non-certifiable/non-testable behaviors that are desirable in software development, hardware development, deployment, testing, and hardening areas.