Before the
National Institute of Standards and Technology
DEPARTMENT OF COMMERCE
Washington, D.C. 20230

In the Matter of	)	
	)	
Recommendations for IoT Device	)	NISTIR 8259
Manufacturers: Foundational Activities	)	
and Core Device Cybersecurity Capability	)	
Baseline (2nd Draft)	)	

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").[1] To further enhance credibility and adoption, OCF has successfully worked with ISO/IEC to have the OCF specification adopted as ISO/IEC standards.[2] 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

[1] The full OCF specification is available at https://openconnectivity.org/developer/specifications/; details on the certification process can be found at https://openconnectivity.org/certification/ocf-certification; and the OCF open source reference implementation, IoTivity, is available at https://iotivity.org/.

[2] 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.

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 continues to support NIST's ongoing efforts to increase the security of IoT devices, both in this proceeding and more generally. In September, OCF filed comments with NIST in response to the first draft of NISTIR 8259.[4] OCF agrees with many of the changes NIST has incorporated in the second draft of NISTIR 8259 and submits these comments to help continue to refine the report. Specifically, OCF agrees with the inclusion of third-party references as part of the core baseline and requests that NIST include OCF as a further implementing reference. OCF goes beyond guidance and provides an example implementation of the capabilities identified in the Core Baseline. More fundamentally, NIST should publish the Core Baseline as a standalone document, separate and apart from the Foundational Activities to avoid confusion, potentially weakening the message of the baseline. Lastly, OCF supports the increased flexibility in the newly proposed "Cybersecurity State Awareness" core baseline capability and encourages NIST to work closely with industry to ensure this nascent capability is adopted in a manner that meaningfully improves device security.

II. DISCUSSION

a. OCF Requests that NIST Include the OCF Specification in the Core Baseline as an Implementing Reference

OCF strongly supports NIST including third-party references as part of the Core Baseline.[5] As NIST explains, the last column in the Core Baseline provides a list of IoT reference examples to help the reader understand each capability in more detail and to learn

[3] Membership List, Open Connectivity Foundation, https://openconnectivity.org/foundation/membershiplist.

[4] Comments of the Open Connectivity Foundation, In the Matter of Core Cybersecurity Feature Baseline for Securable IoT Devices, Draft NISTIR 8259 (Sept. 30, 2019), available at https://openconnectivity.org/wp-content/uploads/2019/10/OCF-NIST-comments-final-093019.pdf.

[5] Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline, Draft (2nd) NISTIR 8259, NIST 11-12 (Jan. 2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259-draft2.pdf.

how "to implement each capability in a reasonable manner."[6] OCF encourages NIST to be expansive in its inclusion of implementing references to make clear that the identified core baseline capabilities are widely, readily, and easily available to IoT manufactures. To that end, OCF requests that NIST include the OCF Specification as a further reference to provide the reader with an example implementation of the identified capabilities.

The currently included references provide valuable guidance – this is particularly true of the references to the CSDE,[7] but largely lack specific examples of how to implement the Core Baseline capabilities. Unlike the currently included references, OCF provides an *actual* implementation that provides an example of how to incorporate the capabilities identified in the Core Baseline. Moreover, not only does OCF provide a specification implementing these capabilities, but OCF also provides open source reference software, the actual *code*, that implements the OCF specification including the Core Baseline capabilities.[8] To be clear, both the OCF Specification and the associated open source reference implementation are freely available to anyone.[9] Including references to OCF will enhance and deepen the understanding of the Core Baseline by providing the reader with an example implementation developed through the consensus of a broad cross-section of the IoT industry – OCF's over 450 member organizations – and recognized as a global standard by ISO/IEC.

Since our prior comments in this proceeding, OCF has continued to advance its secure interoperability specification and in lockstep, its open source reference implementation. For ease of reference, OCF has included as Attachment 1 an updated mapping of the current

[6] *Id*. at 11.

[7] OCF actively contributed to the development of the C2 Consensus on IoT Device Security Baseline Capabilities. *See 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] OCF sponsors the Linux Foundation Collaborative Project, "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 and capabilities identified in the NIST Core Baseline. *See* IoTivity, available at https://iotivity.org/.

[9] The value of OCF membership is in significant part the ability to influence and contribute to the future direction of OCF as well as gaining access to the OCF certification program.

standard to the updated Core Baseline. As the mapping shows, OCF now supports all six core capabilities identified in the baseline. OCF requests that NIST incorporate these references in the final Core Baseline to provide the reader with a deeper understanding of how to potentially incorporate the capabilities identified in the Core Baseline.

III. NIST Should Publish the Core Baseline as a Standalone Document, Separate and Apart from the Foundational Activities

NIST seeks to use a single report, NISTIR 8259, to address two distinct action items from the Botnet Road Map: (i) to create a baseline of cybersecurity capabilities for IoT devices, and (ii) to publish cybersecurity practices for IoT device manufacturers.[10] OCF is concerned that by attempting to combine these two actions – a Core Baseline and Foundational Activities – there is a potential to create confusion and to weaken the potential positive impact of the Core Baseline in increasing the security of IoT devices broadly. The current structure of NISTIR 8259 weakens the perceived importance of the Core Baseline by placing it within a Foundational Activity rather than emphasizing the standalone importance of the Core Baseline as the set of capabilities that all IoT devices should incorporate. More specifically, NIST currently has the Core Baseline framed as a means of addressing the customer's "cybersecurity goals." Although the Core Baseline may be used to support a specific customer's cybersecurity goals, the Core Baseline supports and helps further the broader purpose of ensuring resilience of the Internet against botnet attacks by reducing the availability of easily exploitable IoT devices.[11]

In support of this broader purpose, NIST should make clear that the Core Baseline is meant to help ensure that all IoT devices have a minimal set of cybersecurity capabilities to reduce the

[10] Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline, Draft (2nd) NISTIR 8259, NIST at v, note 1 (Jan. 2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259-draft2.pdf.; *see also* A Road Map Toward Resilience Against Botnets, Dept. of Commerce (Nov. 29, 2018), https://www.commerce.gov/sites/default/files/2018-11/Botnet%20Road%20Map%20112918%20for%20posting_0.pdf.

[11] *See generally* A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats, Dept. of Commerce & Dept. of Homeland Security (May 22, 2018), https://www.commerce.gov/sites/default/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf.

risk of attackers exploiting those devices for use in botnets. By separating out the Core Baseline from the Foundation Activities, NIST would eliminate the opportunity for confusion and avoid blurring the necessary and needed distinction between baseline capabilities of devices and foundational activities of the business and increase the impact of both elements. Separating out the Core Baseline from the Foundational Activities will increase the likelihood that device manufacturers will adopt the Core Baseline and incorporate those capabilities into each and every IoT device. As currently structured, NIST risks signaling or setting the perceived expectation that IoT manufactures should only adopt the core baseline as part of incorporating the Foundational Activities. OCF encourages NIST to make clear that even if an IoT manufacturer is unable to adopt the full range of Foundational Activities that the Core Baseline can and should be adopted. In order to provide this clarity, OCF suggests that NIST position the Core Baseline as a critical first and standalone step in increasing IoT device security.

Moreover, the proposed Foundational Activities are directed towards an inherently different purpose and scope from the proposed Core Baseline such that their clear delineation as separate steps would increase their respective impact and likelihood of adoption by industry. The Foundational Activities provide guidance on the business processes of the IoT manufacture. In comparison, the Core Baseline provides a minimum set of cybersecurity capabilities for an IoT device. Recognizing this fundamental difference in purpose, NIST should separate the Core Baseline and Foundation Activates aspects of NISTIR 8259 into separate reports or at minimum, elevate the Core Baseline as separate and standalone section within NISTIR 8259 and make clear this is a minimum set of capabilities applicable to all IoT devices. Such a restructuring of the report will also help to reduce the risk that the Foundational Activities and Core Baseline will be treated similarly by legislative bodies and other government agencies.

IV. OCF Supports the Increased Flexibility in the Newly Proposed "Cybersecurity State Awareness," and Encourages NIST to Work Closely with Industry to Ensure Effective Adoption of this Core Capability

OCF agrees with NIST and fully supports the increased flexibility with the newly proposed "Cybersecurity State Awareness" core capability and the recognition that "Cybersecurity Event Logging" is not a capability that is necessarily appropriate for all IoT devices and deployments. The current OCF Specification as well as the open source reference implementation provides a device with the ability to report on its cybersecurity state, to differentiate between a normal and degraded state, and to restrict access to this information to authorized entities, as set forth below in Attachment 1.

Relatedly, OCF is nearing completion of incorporating support for cybersecurity event logging into its specification and open source reference implementation. Once completed, this addition will enable support for capabilities above and beyond the Core Baseline capability of "Cybersecurity State Awareness" and further demonstrates OCF's ongoing commitment to continually driving increased device security. To date, OCF has developed the draft specifications supporting event logging and has released those drafts publicly as part of the normal intellectual property rights (IPR) review process.[12] OCF anticipates these draft specifications will become part of the full OCF Specification in the next couple of months. At which time, event logging will also be supported and available in the OCF open source reference implementation.

[12] OCF's draft specifications currently under IPR review can be found at https://openconnectivity.org/developer/specifications/draft-specifications/. The specific changes to provide support for event logging are found in the following draft specifications: (1) "Event Logging for OCF Devices," https://openconnectivity.org/draftspecs/Gaborone/CR%203035%20-%20Event%20Logging.pdf; (2) "New Resource Type for Event Logging," https://openconnectivity.org/draftspecs/Gaborone/CR%203149%20-%20New%20Resource%20Type%20for%20Event%20Logging.pdf; (3) "New Resource Type for Event Logging" (List of Auditable Events), https://openconnectivity.org/draftspecs/Gaborone/CR%203150%20-%20List%20of%20Auditable%20Events.pdf.

Outside of the process of developing NISTIR 8259, OCF encourages NIST to work with industry to develop further detailed practical guidance on the implementation of this capability. Unlike the other identified Core Baseline capabilities where implementations and tradeoffs in an IoT context are more widely understood, “Cybersecurity State Awareness” is a nascent capability and the industry could benefit from NIST’s further guidance in implementing this feature to ensure the various tradeoffs are fully considered and that this capability is incorporated in a manner that meaningfully increases the security of IoT devices.

V. CONCLUSION

OCF continues to support NIST’s work in IoT security and in particular its development of NISTIR 8259. Specifically, OCF supports including third-party references as part of the Core Baseline and requests that NIST include OCF as a further implementing reference. OCF is concerned that the current structure of the NISTIR 8259 weakens the Core Baseline and suggests that NIST separate the baseline from the Foundational Activities. Lastly, OCF supports the increased flexibility in the newly proposed “Cybersecurity State Awareness” baseline capability and encourages NIST to work closely with industry to ensure this nascent capability is adopted in a manner that meaningfully improves device security.

Should NIST have any questions in relation to these comments, please contact Mark 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

Kelton Shockey
Strategy Specialist, Technology Policy, CableLabs

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

February 7, 2020

ATTACHMENT 1:

Mapping of OCF Specification to the NISTIR 8259 “Core Baseline”

OCF continues to revise and expand its specification and open source reference implementation. To ensure access to the most accurate and up-to-date information, please visit https://openconnectivity.org.

NIST Device Cybersecurity Capability	Key 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 at an external or internal location on the device authorized entities can access Note: the physical and logical identifiers may represent the same value, but they do not have to.	**[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 PKI participants and Certification Authorities (CAs).
Device Configuration: The configuration of the IoT device’s software and firmware 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 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 Device Cybersecurity Capability	Key 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 demonstrably secure cryptographic modules for standardized 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 entitiesto 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) 3. Configuration settings for use with the Device Configuration capability including, but not limited to, the ability for authorized entities to configure the cryptography use itself, such as choosing a key length	**[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 that the 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 Interfaces: The IoT device can restrict logical access to its local and network interfaces, and the protocols and services used by those 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. Configuration settings for use with the **Device Configuration** capability including, but not limited to, 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.

NIST Device Cybersecurity Capability	Key Elements	OCF Reference
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 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 for authorized entities to roll back updated software and firmware to a previous version 4. The ability to restrict updating actions to authorized entities only 5. The ability to enable or disable updating 6. Configuration settings for use with the Device Configuration capability including, but not limited to: a. The ability to configure remote update mechanisms to be either automatically or manually initiated for update downloads and installations b. 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).
Cybersecurity State Awareness: The IoT device can report on its cybersecurity state and make that information accessible to authorized entities only.	1. The ability to report the device's cybersecurity state 2. The ability to differentiate between when a device will likely operate as expected from when it may be in a degraded cybersecurity state 3. The ability to restrict access to the state indicator so only authorized entities can view it 4. The ability to prevent any entities (authorized or unauthorized) from editing the state except for the device's monitor 5. The ability to make the state information available to a service on another device, such as an event/state log server	**ISO/IEC 30118-2:2018] Clause 13.10:** Security Virtual Resources (SVRs) and Access Policy **ISO/IEC 30118-2:2018] Clause 8.6:** Device enters state SRESET when in a non-operational, degraded state. **ISO/IEC 30118-2:2018] Clause 5.1:** Describes access control architecture and the access based on state of device. **ISO/IEC 30118-2:2018] Clause 12:** Access control is enforced over all Resources.