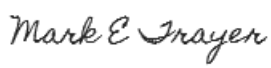
October 15th, 2021

To: labeling-eo@nist.gov

The Open Connectivity Foundation (OCF) respectfully submits the attached document detailing comments regarding the DRAFT Baseline Security Criteria for Consumer IoT Devices.

If you have any questions, please contact staff@openconnectivity.org.

Regards,



Mark Trayer
Chairman of the Board, Open Connectivity Foundation

Open Connectivity Foundation
3855 SW 153rd Drive, Beaverton, OR 97003 U.S.A.
TEL: (503) 619-0673 https://openconnectivity.org/

The Open Connectivity Foundation (OCF) has mapped several of the IoT security baselines with the set of specifications that comprise the OCF IoT Specification. We have found that our specification aligns favorably with many baselines published by both industry and government entities, including both NISTR 8259A and the draft NISTIR 8259D. The notable exceptions to this are aspects of baselines that are more broadly scoped than a device specification can cover, for example how a vendor handles end-user data in their perspective cloud implementations is outside of the purview of the device and protocol focused OCF specification.

Our specific comments on the whitepaper draft, "Baseline Security Criteria for Consumer IoT Devices" are as follows:

1. Whether these are appropriate criteria for a broad range of consumer devices

OCF: Table 1 is adequately focused on the definition of the IoT product and is appropriately scoped to consumer IoT devices.

2. Whether additional criteria are needed, including criteria that specifically address other components of the product beyond the device

OCF: Given the heterogeneity of IoT ecosystems, components, and capabilities addressing components of the IoT product beyond the device may be infeasible.

3. Whether Tables 1, 2, and 3 have the right level of detail in the discussion of the criteria to ensure consistency in meeting the cybersecurity expectations

OCF: Table 1 is adequately focused on the definition of the IoT product and is appropriately scoped to consumer IoT devices.

OCF: Table 2 may be more clearly defined as the vendor ecosystem supporting capabilities and criteria.

4. What might be the appropriate definitive text for these criteria be stated to facilitate conformity assessment

OCF: Table 1- Capability logical Access to Interfaces #4:
   - *" The ability to authenticate individuals and other IoT product components using appropriate mechanism to technology, risk and use case. Authenticators could be biometrics, passwords, etc."*
   - *Comment: Separate these criteria into two distinct clauses,*
     - *The authentication of individuals where authenticators can be biometrics*
     - *The authentication of IoT product components where authenticators can be machine to machine directed.*

5. The extent to which consumer IoT devices with very limited capabilities (e.g., microcontroller-based devices) can address the criteria

OCF: Microcontroller-based devices should have the same levels required criteria as other non-limited devices as threats and risks are often the same between constrained and non-constrained devices.

6. The potential for assessment and certification of IoT product components (e.g., cloud backend, hub, mobile app) independent of one another

OCF: The Open Connectivity Foundation current certifies cloud, mobile app and device independently from one another. Here again the heterogeneity of IoT ecosystems may make certifying ecosystems as a whole infeasible.