**Philips COMMENTS**

# NIST Draft white paper with draft criteria for a labeling program on cybersecurity capabilities of Internet-of-Things (IoT) devices

**COMMENTER:** Philips

We appreciate an opportunity to comment on this draft, "Baseline Security Criteria for Consumer IoT Devices," as an important step towards greater cybersecurity in critical sectors like healthcare.

Line(s) No. – *Line number of the guidance on which you are commenting* – **N/A, no line numbers are available in the paper under review.**

| Line Number | Section / Table Name | Page Number | Comment |
|---|---|---|---|
| N/A | General comment on document. | N/A | In future documents that seek feedback, please include line numbers so it is easier to comment on specific line items. |
| N/A | General comment on document. | N/A | It is imperative that the scope of devices that come under the purview of these documents be very clearly and distinctly identified. There are many devices that fall under IoT space that also fall under highly regulated device categories for e.g., medical devices. Please consider that IoT medical devices are already highly regulated, and in the USA, FDA is increasingly and stringently focusing on cybersecurity characteristics of such devices as part of the clearance process to ensure safe and effective operation is maintained across the device lifecycle. Mandating additional labeling requirements on such devices by other government entities increases burdens on manufacturers of such devices; these IoT medical devices already need to meet stringent labeling requirements due to the presence of global regulations that also cover cybersecurity related labeling / information provision (E.g., FDA, EU MDR/IVDR etc.). |
| N/A | General comment on document. | N/A | Since a hard label merely represents a snapshot in time, we strongly agree that this effort should encourage innovation in manufacturers' IoT security efforts, leaving room for changes in technologies and the security landscape. This includes allowing flexibility in implementation, including use of digital labels. |
| N/A | General comment on document. | N/A | IoT labeling should be practical and not be burdensome to manufacturers and distributors. This include advocating for reciprocity/recognition and harmonization of Iot security labels that are being or going to be required across different countries. We hope NIST uses its resources as an entity of the US. Government to advocate for this position of harmonization / consensus. |

**Philips COMMENTS**

# NIST Draft white paper with draft criteria for a labeling program on cybersecurity capabilities of Internet-of-Things (IoT) devices

| Line Number | Section / Table Name | Page Number | Comment |
|---|---|---|---|
| N/A | General comment on document. | N/A | Any labeling program should factor in usability, UI and human factors aspects as important considerations. |
| N/A | General comment on document. | N/A | The initiative should build on national and international experience of existing programs. |
| N/A | General comment on document. | N/A | Allow for diversity of approaches and solutions across industries, verticals, and use cases – so long as they are deemed useful and effective for consumers. Allow for a framework that allows for self-attestation as well as third party attestation as part of conformity assessment. |
| N/A | General comment on document. | N/A | Since there is no one size fits all and not all Iot devices are the same, any labeling program should adopt a risk based tiered/layered approach, with device and products posing a greater risk in the event of a security breach be required to fulfill more requirements than those that pose a reduced risk or minimal. |
| N/A | General comment on document. | N/A | Any labeling framework that is developed should clearly delineate scope, and whether labeling criteria apply to just a device or the entire device ecosystem for e.g., hubs, backends, clouds, associated SW apps etc. Our recommendation is that the labeling program be restricted to devices since the ecosystem of supporting/enabling features are not always controlled / developed by the same manufacturer developing the IoT device. The document should be further clarified to highlight the need for any labelling program to be suited to its intended purpose. Concrete device examples would also help readers understand the spectrum of devices this labelling criteria is intended to cover. |
| N/A | Table 1 – Logical Access to Interfaces | 4 | Include additional criteria of audit trail either at the device or the back-end. Audit trail should be part of Access control as an "after the fact control" |
| N/A | Table 1 – Software Update | 4 | Audit trail as after the fact control. |
| N/A | Table 1 – Product Security | 5 | Clarify if this is regarding Product Security of Product Resilience |
| N/A | Table 2- Information and Query Reception: | 7 | Should the manufacturer only be reactive or also proactively monitor the software and other tooling used in the solutions and take appropriate action? |
| N/A | Table 3 – Product Security | 9 | This is better identified as Product Resilience instead of Product Security |
| N/A | Criteria for Label<br>• Actionable by the consumer | 11 | Just a statement attesting that the security of the device/product complies with the level needed for the intended purpose will not be enough. This is because there will be grey areas of controls implemented that are different than tested or self-evaluated. |

**Philips COMMENTS**

**NIST Draft white paper with draft criteria for a labeling program on cybersecurity capabilities of Internet-of-Things (IoT) devices**

| Line Number | Section / Table Name | Page Number | Comment |
|---|---|---|---|
| | | | |
| N/A | Criteria for Label<br>• Effective in conveying the product's value | 11 | It is very important to be able to relate what is stated here to the intended use and the lifecycle use of the product. e.g. Security controls that are expected to be base level 5 years from now but are not currently in place. (e.g. Encrypted IPC communication within a IOT device) |