SUBMITTED ELECTRONICALLY VIA E-MAIL

October 18, 2021

Subject: UL Comments on NIST DRAFT Baseline Security Criteria for Consumer IoT Devices

U.S Department of Commerce
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

To Whom It May Concern:

UL appreciates the opportunity to review NIST's draft Baseline Security Criteria for Consumer IoT Devices and submit these comments to enhance NIST's efforts. UL previously submitted comments on this issue in September of 2019 on the Draft NISTIR 8259, *Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers* and again in February on *NIST's IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements.* These comments build off of those submissions and address feedback directly related to NIST's execution of President Biden's Executive Order 14028, "Improving the National's Cybersecurity", specifically sections 4 (s) and 4 (t) that calls for NIST to initiate pilot consumer labeling programs for IoT cybersecurity of devices and software development practices.

Since its inception in 1894, UL has served a mission of promoting safe living and working environments for people everywhere and continues to fulfill our promise of facilitating the flow of goods across borders. Grounded in science and collaboration, UL's work empowers trust in pioneering technologies, from electricity to the internet. We help innovators create safer, more secure products and technologies to enable their safe adoption.

UL believes that third party assessment and verification is crucial in the effort to securing device cybersecurity. Product testing and verification or certification by independent third parties – along with the attachment of a visible well-known mark – provides confidence that devices will function according to manufacturers' intentions and instructions, as well as comply with industry and government specifications and requirements. The ability of device manufacturers to credibly demonstrate the performance, safety and security of their systems will be critical to establishing trustworthiness and should serve two purposes: 1) to help manufacturers and developers improve the security posture of their products by leveraging proven 'security best practices', and 2) to rate the security posture of IoT solutions in order to make security more transparent and accessible to end users.

UL has been leading or instrumental in developing several cybersecurity/risk management standards and frameworks to address IoT device and ecosystem cybersecurity risk and protection, and taking these forward in assessment, verification, certification and labeling programs or solutions that are voluntary, rely on market driven mechanisms, and are risk management-based and internationally aligned. Among these is *UL Methodology for Marketing Claim Verification: Security Capabilities Verified to level Bronze/Silver/Gold/Platinum/Diamond, UL MCV 1376*. Additionally, UL has led development of *UL 5500: Standard for Safety for Remote Software Updates* and evaluation and certification to the standard, which is designed to set criteria for OTA (over the air) safety software updates. UL has also led or been instrumental in developing UL 2900 and IEC 62443 series of standards and evaluation and certification schemes.

As NIST moves forward with its efforts to initiate the two pilot programs called for in EO 14028, UL is eager to share our valuable expertise, including our experience as a testing and certification body in similar government-led, labeling efforts around consumer-facing issues such as energy efficiency [EPA's ENERGY STAR® program], electrical safety [OSHA's Nationally Recognized Testing Laboratory (NRTL) Program], and sustainability (EPA's Environmentally Preferable Purchasing Program Pilot). If you have any questions regarding this submission or would like to discuss UL's recommendations further, please do not hesitate to contact Amanda Kalyan, UL Global Government Affairs, at Amanda.Kalyan@ul.com. Thank you for your attention to these comments.

Respectfully,

Derek Greenauer
Director, Global Government Affairs
UL LLC

General Observations:

NIST's draft Baseline Security Criteria for Consumer IoT Devices cites "three dimensions of a consumer Internet of Things (IoT) cybersecurity labeling program" that must be addressed:

1. Baseline security criteria,
2. Conformity Assessment criteria, and
3. The label.

During the workshop on September 14 and 15, participants, including multiple from UL, seemed to have a number of unanswered questions on some foundational elements of the effort that NIST has been tasked with. UL believes that NIST needs to answer those foundational questions before diving too deep into the specifics of the three dimensions of a IoT cybersecurity labeling program. Those foundational issues that should be addressed prior to establishing any kind of pilot program are:

Who is the "Consumer"? Who is the audience for the label?
Defining who the audience is a critical first step. It helps to narrow down into audience sectors as not all audiences have the same level of expectations, technical acumen, or needs. For instance, a retired grandmother who wants a secure product to use to see her grandchildren will have different needs and expectations of what a label should communicate than a technology buyer for a big-box retailer.

Once a "Consumer" is clearly defined, the next recommendation is to develop a problem statement.

What is the specific problem that this labeling pilot is going to be developed to overcome? What metrics are needed to determine progress? When ENERGY STAR was first developed, it was meant to be a market transformation program, giving consumers an easy way to identify a product that had been recognized to use less energy than other, non-marked products. Over time, ENERGY STAR developed metrics to measure their progress -- % of sales that are ENERGY STAR qualified versus standard products; Consumer awareness of the ENERGY STAR mark over time; and finally, energy savings achieved.

With a knowledge of who the audience is for the labeling program and what is going to be achieved through a labeling program, you can then begin to build out specifics such as:

What is the scope of the Consumer IoT Device labeling pilot?
Since it is a pilot, UL recommends starting with a narrow scope and building out over time with the benefit of learning lessons along the way. ENERGY STAR was born out of another EPA program, Green Lights program in 1991. The following year, ENERGY STAR was created for office equipment, namely computers and displays. In the 30 years since the program was started, EPA leveraged the knowledge gained through these early efforts to add another 63 product categories to the program as well as similar efforts for residential homes, commercial buildings, and industrial plants.

Addressing these questions early, will, in some cases, help inform the direction the pilot programs take, and in other cases, reveal more questions in need of answers.

Specific Technical Comments

IoT Product Cybersecurity Capability and Potential Criteria [Page 3-4, Table 1]: UL believes that many of the potential criteria listed in Table 1 needs to be more clearly defined to include approaches/methods/standards that direct ***how*** these criteria are to be evaluated. Any criteria selected needs to be testable and reproducible across IoT products.

Asset Identification [Page 3, Table 1]: There will need to be detail regarding what qualifies as an identifier for this requirement. As written, it is limited to providing the ability to track the deployment of components. However, "identifiers" are also often used to determine certification/approval status. Example: If the objective is to allow a user to determine the hardware and firmware versions, and certification/approval status, then this is needed somewhere in the criteria.

Data protection [Page 4, Table 1]: UL is supportive of NIST's inclusion and reference to FIPS 140-3. It is one of the few internationally-accepted standards.

Software Updates [Page 4, Table 1]: In line 3, UL recommends removing the phrase "… or disable notifications about updates". It is unclear to UL how allowing a consumer to turn off notifications about software updates enhances that product's security.

Documentation [Page 5, Table 2]: Documentation should include identification of cryptographic algorithms and security protocols as well as cryptographic keys, their use, and size.

Information Dissemination [Page 7, Table 2]: UL believes the consumer would be best served if a product security policy is made available that identifies the types of data handled by the product and what the manufacturer's policies are around what they will do with that data (assuming it is accessible to the manufacturer).

Data Protection [Page 9, Table 3]: The requirement needs to be clarified as to when it would be acceptable to transmit un-encrypted data. Example: is a risk analysis approach used to determine acceptability? Are compensating controls needed to mitigate risks?

Software Update [Page 3, Table 3]: The ability to update the software of **all** IoT product components seems too overly aggressive for a pilot program. UL believes this will be extremely difficult for an IoT device manufacturer to attain as many of their components are legacy in nature. For example, there are hardware bootloaders that cannot be updated because they are in ROM, there are RF baseband chips which cannot be updated, etc.

Increasingly Comprehensive Levels of Testing and Assessment (Tiers) [Page 10, Paragraph 1]: It would be useful to acknowledge that higher levels of security may also (in addition to safety) be needed for devices that handle sensitive private data. The existing safety example is good, but individuals also need to be conscious of IoT risks to personal data as well.

Conformity Assessment Approaches [Page 10, Paragraph 1]: UL cautions NIST on the language in this paragraph as it could be inferred that all three approaches to conformity provide the same level of assurance to a consumer that the IoT product or device meet the criteria behind the program. Ann Bailey's presentation during the Workshop detailed how ENERGY STAR started with a self-attestation approach to conformity at the outset of the program and soon realized that consumers expected higher levels of assurance. EPA realized that the program's reputation with consumers and other stakeholders was dependent on products performing as advertised and thus changed their approach to leverage accredited, private sector third-party testing and certification bodies. NIST should leverage the learnings of EPA at the outset and leverage accredited third parties in these pilots.

Criteria for the Label [Page 11, Paragraph 2]: (Understandable by the Consumer): It is important that "intended use" be disclosed to the consumer in a way that allows them to understand risk. Key aspects should be available to the consumer to foster both good decisions, and IoT awareness. Example questions a consumer should have answers to include: does the device collect and transmit video, does the device access sensitive information from other devices, does the device *generate* sensitive information such as video or audio, does the device allow purchases, and does the device push information to back-end or cloud-based components.