



Via E-mail labeling-ee@nist.gov

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

Subject: [Draft Baseline Criteria for Consumer Software Cybersecurity Labeling](#)

UL respectfully submits these comments in response to NIST's Request for Comments on Consumer Software Labeling with regard to Executive Order (EO) 14028 *Improving the Cybersecurity of the Federal Government*, issued on May 12, 2021. The suggestions and feedback provided by UL are informed by its experience implementing, conducting, and administering multiple security certification programs for IoT devices, a key example of which being the UL Cybersecurity Assurance Program (CAP). CAP certification is particularly relevant to the topic of software labeling as ANSI/CAN/UL 2900 (a series of standards for Software Cybersecurity for Network-Connectable Devices) serves as the benchmark against which products and software are evaluated.

The suggestions and feedback provided below are summarized under three main categories: outcome, label and deployment. UL believes these three categories help to focus the intent and purpose of this section of the EO. Comments to NIST's specific questions follow this initial discussion.

More generally, UL believes NIST should approach this program from the view of the consumer, keeping in mind that the average consumer is not fully aware of all the complex, technical issues surrounding cybersecurity. If the purpose is ultimately to have the consumer "feel better" about a product because it bears a cybersecurity label, then the process and outcome should be driven for the consumer.

I. OUTCOME – what does NIST want to get out of this labeling program?

From NIST's draft, we assume that NIST is attempting to develop a baseline set of criteria from which to evaluate a software product in order to give confidence to a consumer that the product is "cyber safe". If the product meets that baseline, or potentially is higher, it will be given a label. The issue associated with the goal of the outcome is what criteria should be used for evaluation and how products should be evaluated it is evaluated to meet such criteria, in this case NIST's use of self-attestation.

In UL's experience, assessment approaches using vendor attestation have significant weaknesses. Vendors often lack expertise, knowledge or skills in security concepts and assessment practices and can misinterpret basic requirements without support. A significant benefit to third-party assessment approaches is the education provided to the developer community through interaction during the assessment process. Even a low assurance assessment approach involving a third-party assessor, where minimal testing is performed, provides tremendous value to developers and consumers by providing an objective, independent review to ensure that developers have a consistent interpretation of security concepts and requirements across industries.

In addition, UL questions the "pass/fail" approach and recommends using a tiered approach. In a pass/fail, the consumer may not know the extent to which the product has met criteria. For example, if the product is given a 3/5 rating, the consumer can know that the product is relatively safe but must have some vulnerabilities that consumer must investigate further. Underwriter Laboratories standards development process is a consensus-based approach utilizing input from a broad range of stakeholders. The diverse stakeholders that make up the standards technical panel for ANSI/CAN UL

2900/ [MD2] [BD3] determined that the general requirements of the standard would serve some markets better by offering a three-tiered approach with increasing requirements and security for each subsequent level. The resulting standard of ANSI/CAN/UL 2900-2-3, was readily adopted into UL CAP. Certificates are issued reflecting the level of requirements to which the software was successfully tested. Another option would be that a lower tier might be suitable for the Supplier's Declaration of Conformity (SDoC) whereas the higher tiers should involve third party. We think this is a reasonable approach that allows the makers of very simple products to avoid third-party expenses. However, the makers of complex products, which would need independent confirmation (especially if risk management is assessed), would have another layer of credibility and security.

UL has also developed the UL MCV 1376 Methodologies (IOT Security Rating Program for consumer IOT Devices [MD4]), enabling security levels **and is also compliant (Level 3+)** to the EN 303 645 standard (also adopted as the baseline for Singapore's National Cybersecurity Labelling Scheme (CLS)). UL MCV 1376 also references a number of other governance frameworks to enable compliance for different products for various use-cases, and increasing the level of assurance based on sensitivity of devices e.g. Baby Monitors/CCTV Cameras require a higher level of assurance as opposed to a smart blender. The program includes an annual surveillance deployment.

UL would like to see a more defined scope of this program as it needs a better definition of exactly what categories of products are in scope and the types of software that are applicable. Providing examples would be helpful. Perhaps the scope as currently defined is too large, and a smaller pilot program would be advisable for a start. NIST could begin with a confined group and assess its success or make adjustments as it is deployed before opening it to entire software market.

Finally, with regard to the technical criteria needed to support consumer software security assertions, ANSI/CAN UL 2900 series of standards as well as ULMCV1376 require the developer to have implemented and used risk management processes throughout the software/product life cycle. These certifications require third-party examination of documentation describing the risk management process. Third-party code analysis and penetration testing is used to identify software vulnerabilities and weaknesses, which are submitted to the developer to be addressed under their risk management process. The results are reviewed by the third-party tester to verify that effective remediation, typically including software updates, has occurred. This process provides assurance that the risk management process will be effective throughout the product life cycle and that newly discovered vulnerabilities will be effectively addressed for fielded and newly deployed devices.

Whether testing software cybersecurity, or security controls for device safety, as is done under UL 5500 testing, it is important that the software is controlled under a documented system for software identification and versioning that is sufficient for identifying all critical software used to implement security controls. Verifying this is key to ensuring that the scope of testing is correct, and the certificate (labeling) clearly identifies the critical software so that products that have undergone certification can be distinguished from similar products that are not. To support consumer identification of certified software, testing can be performed to verify that a product provides a means to identify to a user the software that is currently running.

II. LABEL – Who develops and executes the label and what does it mean?

NIST will need to identify what entity or issuing authority that will be tasked (authorized) to develop/design the actual label and monitor the product post labeling.

Should the label used include a QR code/Verification ID that send the consumer to a FAQ or other fact sheet regarding the security particulars, the information provided should be a clear, concise and easy to understand template that applies across the board – providing constancy and quality. E.g. A Smart Control Switch certified as Level 3 Gold on our UL MCV 1376 IOT- Security rating Program: <https://verify.ul.com/verifications/493>

Coupling the binary label with a layered approach will work well with third-party testers. An important topic that will need to be addressed is what entities are authorized to grant the use of a label when third parties are involved. If an appropriate third-party lab performing testing and certification is trusted by the TBD labeling authority, it could be beneficial from an efficiency standpoint, as well as incentivizing the use of third-party test labs, if test labs are able to authorize the use of a label for products they verify to meet the baseline criteria. UL recognizes that this would not obviate the need for the required self-declarations to be provided to the appropriate labeling authority.

III. DEPLOYMENT – How will NIST deploy and execute this program and define what success looks like?

UL would like to know if and how NIST will manage ongoing compliance of products after initial application of label? Under SDoC, providers might “forget” to reassess and re-label their product as changes are made and new vulnerabilities are identified. When critical security updates are made to a product, there will be products in the supply chain that have not received the update. At a minimum, the consumer must be made aware that the product must be updated with the latest software updates in order for the label to be valid.

Also, as mentioned above, UL recommends an initial small, pilot-like deployment of its labeling program as a way to “test” the process before it is deployed widely. Should any hiccups or problems arise, it will be easier and less disruptive to discover them with a closed group of consumers and will allow NIST to make the necessary adjustments before rolling out the labeling program globally. Lastly, UL recommends providing concrete examples of how this program will work, using both simple and complex situations. This information will assist potential commenters in the development of detailed recommendations to NIST.

IV. UL’s Responses to NIST Specific Requests

NIST seeks comments on all aspects of the criteria contained in this draft document, including:

- **Whether criteria will achieve the goals of the EO by increasing consumer awareness and information and will help to improve the cybersecurity of software which they purchase and use.**

UL: Yes, but there will need to be consistency from label to label. This is something NIST notes is out of scope for the draft criteria. If content is the same, but labels diverge in appearance, it will further complicate acceptance and use of the labels by consumers.

- **Whether the criteria will enable and encourage software providers to improve the cybersecurity aspects of their products and the information they make available to consumers.**

UL: The program can have the desired effect if developers perceive it as a competitive advantage. Consumers will have to be perceived as having a positive bias toward products that carry a label.

- **Whether the labeling-specific criteria are appropriate and likely to be effective for consumers.**

UL: Yes, however, consumer education on how to use the label will be important for the criteria to be effective. Unlike a label for nutrition or energy efficiency, many consumers will not have existing knowledge of cybersecurity, or access to cybersecurity experts to assist in understanding and applying the label's information.

- **Whether a single, overarching statement that the software product meets the NIST baseline technical criteria should be included on a label, or whether alternative statements would be appropriate.**

UL: For consumer acceptance, an overarching statement would be most effective, and the statement should be consistently worded for all developers.

- **Whether additional considerations for the labeling approach, consumer education, or testing are needed – including:**

- **Possible appropriate definitive text for describing the labeling program in consumer education materials**

- **Best approaches for addressing the needs of non-English speaking consumers**

UL: For consumers it will be important to have educational material in multiple languages. Multiple formats, such as the use of video demonstrations, will also foster public understanding and benefits from the program.

Educational materials and reference standards describing best practices for conducting testing and adjunct topics such as tool selection are needed to support consistency among developers.

- **Whether the software label approach and design should be unique or extended to the IoT product label (also directed in the EO) to facilitate brand recognition, even though the technical criteria will be different.**

UL: The majority of consumers will not have a deep understanding of the technical criteria. To promote familiarity and label use, the same approach and design should be used for software and IoT products. More sophisticated users will readily understand that the criteria is different and should not be hindered by the labels being similar in appearance.

- **Whether the conformity assessment provisions are appropriate.**

UL: Yes. They capture the key elements that will be needed for consumer use.

- **Whether a template Declaration of Conformity would be useful for software providers.**

UL: Yes. This will promote consistency among developers, aid in the review of the declarations, help reduce omissions, and, if made available to consumers, facilitate consistent interpretation.

- **Whether more details on evidence required to support assertions would be useful for software providers.**

UL: Yes. This will help promote consistency and help developers understand the criteria as well as minimum due diligence on their part when providing attestation.

- **Whether the technical baseline criteria are appropriate, including but not limited to:**

- **The feasibility, clarity, completeness, and appropriateness of attestations**

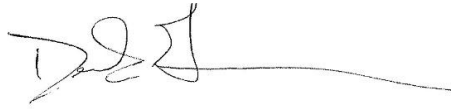
- **Normative references to be considered for inclusion**

- **Potentially requiring that the Software Identifiers attestation take the form of a Software ID Tags**

UL: The baseline criteria are appropriate, but additional guidance and education for developers will be useful to promote consistent application of the baseline.

UL is grateful for the opportunity to provide these comments and is available at any time to discuss these recommendations if desired. Please do not hesitate to contact me with any questions or additional requests for information. Please direct any comments or questions to Amanda Kalyan at Amanda.kalyan@ul.com.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Derek Greenauer', followed by a long horizontal line extending to the right.

Derek Greenauer
Director, Global Government Affairs
UL LLC