SUBMITTED ELECTRONICALLY VIA: LABELING-EO@NIST.GOV

August 17, 2021

Subject: Suggestions and Feedback on Challenges and Practical Approaches to Consumer Software Labeling

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

UL respectfully submits this paper in response to NIST's Call for Papers on Consumer Software Labeling to support of assignments expressed in the Executive Order (EO) 14028 Improving the Cybersecurity of the Federal Government, issued on May 12, 2021. The suggestions and feedback provided in this paper are anticipated to facilitate discussion at the upcoming workshop on Cybersecurity Labeling for Internet of Things (IoT) Devices and Consumer Software, to be held on September 14-15, 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 grouped under the list of challenges (bold and italicized for readability) that are identified in NIST's call for papers.

Formal and informal processes and practices used to secure the software development process

- ANSI/CAN/UL 2900-2-1 requires developers to have implemented and use secure coding practices. These requirements are verified during third-party testing by examination of developer documentation under the CAP certification process.

Technical criteria needed to support validation of consumer software security assertions that reflect a baseline level of secure practices

- ANSI/CAN/UL 2900 series of standards require the developer to have implemented and use risk management processes throughout the software/product life cycle. CAP certification requires 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.

How different conformity assessment approaches (e.g., vendor attestation, third-party conformity assessment) can be employed in consumer software labeling efforts

- Assessment approaches using vendor attestation have significant weaknesses. Vendors often lack expertise in security concepts and assessment practices and can misinterpret basic requirements. 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.

Consumer product labeling programs for educating the public on the security properties of consumer software

- UL's experience with CAP has demonstrated the importance of providing easily accessible certificates that clearly identify the certified software. These certificates provide consumers with the ability to verify that a specific product is certified. Consumers who wish to further understand the certification details are able to view the ANSI/CAN/UL 2900 series of standards at no charge online.

Feasibility and possible means for implementing tiered labels that reflect increasingly comprehensive levels of testing and assessment

- 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 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, ANSI/CAN/UL 2900-2-3, was easily adopted into UL CAP. Certificates are issued reflecting the level of requirements to which the software was successfully tested. It is notable that a key reason a tiered approach was supported by stakeholders, was to facilitate a level of third-party testing that does not require the developer to submit source code as part of the assessment process. Many developers are resistant to providing this very sensitive IP to third parties.

Measures for incentivizing participation by consumer software developers.

- A product software certification approach that allows recognition of component certification will incentivize software developers of consumer products to select certified software sub-components for integration. Consistency of test and certification quality and practices through adherence to ISO 17025 and ISO 17065 are important controls enabling recognition of component certification.

UL welcomes and supports NIST efforts to promote cybersecurity labeling for Internet of Things (IoT) devices and consumer software. We look forward to participating in the upcoming two-day workshop on Cybersecurity Labeling for Internet of Things (IoT) Devices and Consumer Software so that we can share further feedback and suggestions based on our software security testing programs.

Sincerely,

Douglas Biggs
Principle Engineer, UL LLC