ITI Promoting Innovation Worldwide

ITI Comments on Cybersecurity EO's Consumer Software Labeling Program

August 17, 2021

The Information Technology Industry Council (ITI) appreciates the opportunity to submit comments to NIST on consumer software labeling. ITI is the premier global advocate for technology, representing 80 of the world's most innovative companies. Our diverse membership and expert staff provide policymakers the broadest perspective and thought leadership from technology, hardware, software, services, and related industries. ITI welcomes the release of the *Executive Order on Improving the Nation's Cybersecurity*, which delegates NIST to consult with stakeholders to identify secure software development practices and criteria for a consumer software labeling program. ITI emphasizes that ICT products/services, the attack landscape, and knowledge about risks and vulnerabilities are always evolving; therefore, best practices and criteria including those developed pursuant to the EO, should be reviewed regularly. Please find below our comments:

Ensure Labeling Does Not Convey a False Sense of Security

While labels may help incentivize the adoption of the underlying security features, practices, or certifications that they are intended to communicate, they should not be perceived as a substitute for processes to build security and trust, such as secure development lifecycles. In ITI's recently published cybersecurity labeling position paper[1], we state that a label should not indicate that a product is completely secure. Such an assumption would create a false sense of security and could undercut necessary continuous improvement in cybersecurity practices. No label can possibly cover all vectors of attack, new vulnerabilities are continuously being identified, and labels are unlikely to cover the full range of security processes and activities manufacturers and end-users must take to maintain security. Labeling should therefore focus on the highest level of information informed by usability, and it may be more practical to initially focus on particular sector (e.g. consumer IoT software).

Raise End-User Awareness and Balance Responsibility

Any labeling proposal should communicate the policy objective, objective criteria, and the conformity assurance process and associated labeling requirements as clearly as possible. ITI recommends that any labeling program's process, costs, or related certifications should be clear, simple, and reasonable to avoid creating expensive, onerous obligations for manufacturers, discouraging adoption. To raise consumer awareness, ITI recommends NIST communicate the labeling program, engage in usability research, and solicit feedback to assess what is helpful to increase consumer confidence. The goal should be enabling consumers to make intelligent purchasing decisions rather than driving post-purchase behavior. Therefore, similar to nutrition labels, a standardized usable set of easy-to-understand attributes/indexes consistent with software security baseline industry and international standards, which a consumer can easily compare across different products is needed. For example, attributes/indexes may include clear and simple information on secured setup, security updates, network privacy protection (e.g., encryption), secure software features, and attestation. Cybersecurity is a shared responsibility, and manufacturers cannot secure the products and services they develop without other stakeholders' participation. Both consumers and manufacturers must understand their respective roles in maintaining cybersecurity.

Allow Flexible labeling Format and Conduct Periodic Reviews

A cybersecurity "label" should not only be conceived of as a physical sticker, especially in the digital space. Any labeling scheme should be flexible to accommodate a range of formats, including electronic labeling (e-labeling) for digital listings in online marketplaces, machine-readable codes, and other forms of communication that effectively convey the security information to the intended audience. ITI recommends allowing the adoption of e-labels, a digital

[1] ITI Position Paper on Cybersecurity Labeling. April 2021.

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

representation or an electronic means to display regulatory and other important information, which often provides links to a scannable source or internet website that could include information regarding post-purchase recommendations for consumers. E-labeling[2] is one potential way to convey information to end-users and regulators more effectively and efficiently than physical labels. We also encourage adopting the new ISO/IEC 22603 standard for e-labeling policy considerations. We caution against any labeling requirements for unique, specialized, or local features that may create trade barriers or confusing information, and potentially burden companies by causing a fragmented approach to security labeling across different jurisdictions. We further recommend NIST consider conducting periodic reviews to assess the usefulness, effectiveness, and cost of the labeling program, as well as the impact of the labeling on improving security and end- users' decisions. Such assessments can help U.S. government progress toward policy objectives in the cybersecurity EO, make needed adjustments, and better direct resources.

Recognize Conformity Assessments by Suppliers/Vendors and Facilitate Mutual Recognition

We encourage the U.S. government to recognize conformity assessments by vendors, as well as third-party assessment labs, to facilitate the mutual recognition of labeling schemes across international jurisdictions. These approaches also respond to the need for flexibility, agility, and cost limits that must be borne by vendors (and, ultimately, purchasers). Examples of alternative means of attestation include supplier's declaration of conformity (SDoC) and vendor attestation. In addition to recognizing supplier/vendor assessments, we encourage NIST to leverage mutual/multilateral recognition schemes with international partners, such as the International Laboratory Accreditation Cooperation (ILAC) Mutual Recognition Arrangement, the International Accreditation Forum (IAF) Multilateral Recognition Arrangements (MLA), and the Common Criteria Recognition Arrangement (CCRA).

Align with International Standards and Best Practices

We encourage NIST to leverage and align with existing international standards and best practices for software security practices in the process of identifying the baseline security features appropriate to be communicated. These best practices can draw from ISO/IEC 20243:2018 Open Trusted Technology Provider (O-TTPS), SAFECode Fundamental Practices for Secure Software Development, and ISO 27034 Information Technology Security Techniques (also applicable in the context of secure supply chain) ITI also notes the importance of the NIST Software Security Framework, OWASP Software Assurance Maturity Model (SAMM), and Building Security In Maturity Model (BSIMM) as effective frameworks. Although the ISO/IEC 27000 family of standards, ISO/IEC 27001,2 in particular, are not specific to software, they contain basic requirements for an information management system. ISO/IEC 30111 (2019), and 29147 (2018) for coordinated vulnerability disclosure (CVD) are useful resecures for strengthening cybersecurity. ISO/IEC 27402 (in draft) is relevant for baseline software practices for IoT devices.

As NIST looks to develop the software labeling program, NIST should ensure that guidelines do not require companies to unnecessarily disclose information that, if exposed, could put customers at risk. Proposed guidelines, best practices, or standards must be technology-agnostic and account for the risk levels associated with software components that specifically focus on "consumer" products, not business products to protect enterprise software. Such a tiered and narrower approach will help companies tailor the guidelines, best practices or standards to different types of software.[3] Additionally, we emphasize that "best practices" are not one-size-fits-all; some companies have made significant investments in security-first approaches using secure development standards honed over many years. A reference list of useful practices mapped to standards is a helpful tool, but companies should ultimately be afforded the latitude to determine which mix is most appropriate.

[2] ITI Policy Principles of E-labeling. June 2021.