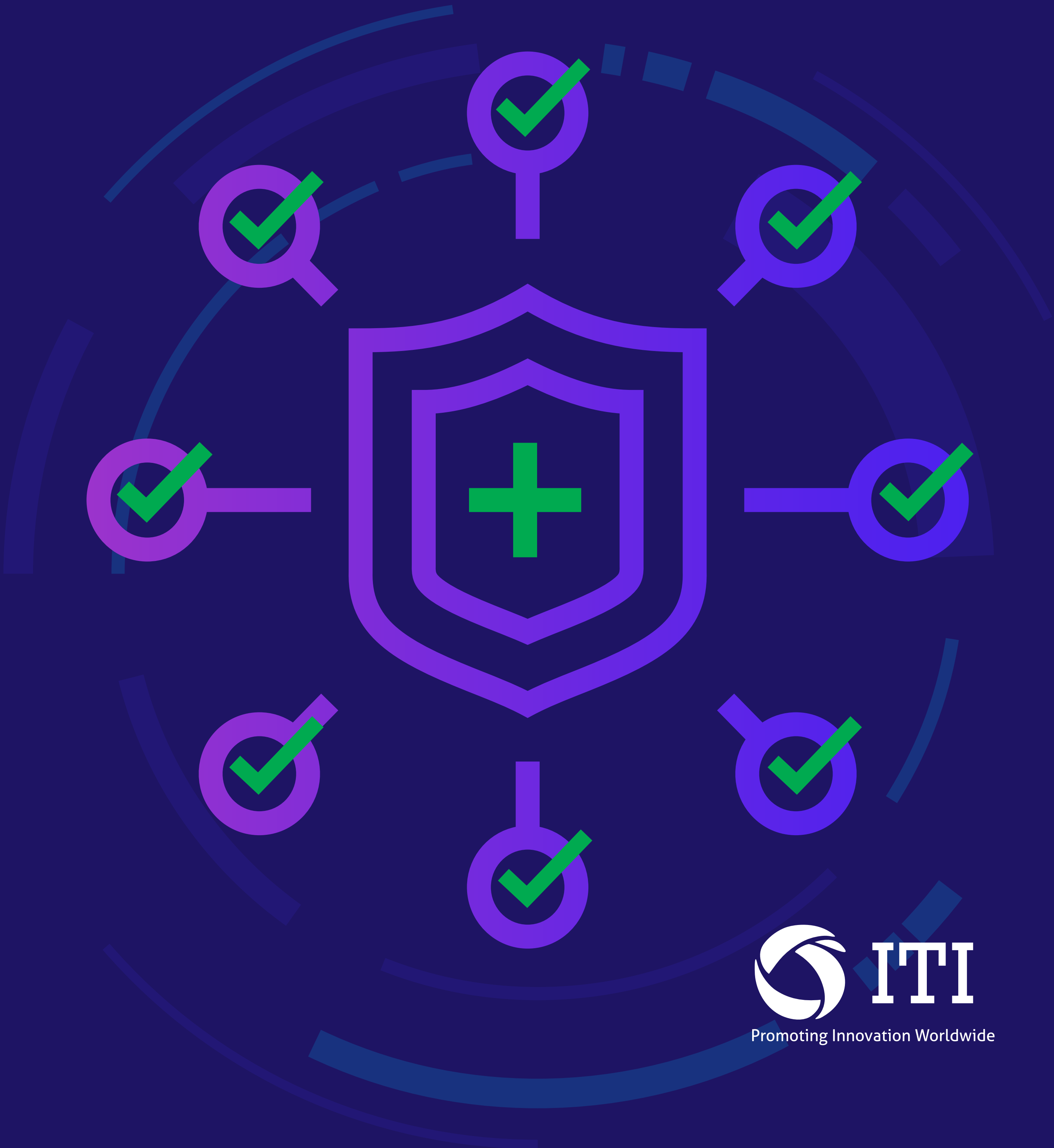
Cybersecurity Labeling:
A Guide for Policymakers

April 2021



ITI
Promoting Innovation Worldwide

The Information Technology Industry Council (ITI) is the premier global advocate for technology, representing the world's most innovative companies. Founded in 1916, ITI is an international trade association with a team of professionals on four continents. We promote public policies and industry standards that advance competition and innovation worldwide. Our diverse membership and expert staff provide policymakers the broadest perspective and thought leadership from technology, hardware, software, services, and related industries.

Governments around the world are considering adopting cybersecurity labeling as a mechanism to better understand and communicate security features in ICT products and services to facilitate confidence, assurance, and trust in such products and services. End-user awareness plays an important role in cybersecurity, and end-users would ideally evaluate device security as a routine part of purchasing. Yet end-users often have limited insight into the presence of security features in a finished product, device or services prior to purchase, which hinders informed buying decisions. Therefore, providing end-users with clear information about companies' adherence to cybersecurity standards and discrete topics such as the security features/functionality in devices or services can foster market competition based on security, build trust, and help end-users fulfill their role in maintaining security.

ITI respects this objective, but at the same time, urges proponents of such proposals to bear in mind that cybersecurity labeling is not a comprehensive or one-size-fits-all solution. While labels may help incentivize the adoption of the underlying security features, practices or certifications they are intended to communicate, they should not be perceived as a substitute for processes intended to build security and trust, such as secure development lifecycles. ITI looks forward to continuing to engage with policymakers on this important topic. Below, we offer our policy positions on security labeling, to better inform those discussions.

Engage Stakeholders, Ensure Clarity, and Balance Responsibilities

- In the process of developing labeling proposals, governments should leverage the expertise of public and private stakeholders and ensure sufficient transparency of such processes. At a minimum, governments should launch public consultations to engage with relevant stakeholders and ensure any new labeling programs add discernible value to end-users and do not create unnecessary barriers to trade, recognizing the global marketplace in which companies are doing business.
- Any labeling proposal should communicate the policy objective, intended audience (such as consumer end-user, enterprise end-user, or regulator), objective criteria, and the conformity assurance process and associated labeling requirements as clearly as possible. Additionally, governments should make clear that labeling is intended to communicate that a finished product or service meets specific security standards at a particular point-in-time.

- ITI recommends governments provide guidance and develop resources for end-users to accompany any labeling program, as doing so can help to raise awareness. Cybersecurity is a shared responsibility, and manufacturers cannot secure the products and services they develop without other stakeholders' participation. Both end-users and operators must understand their respective roles in maintaining cybersecurity. For example, end-users should still protect a "labeled" IoT device with strong WiFi passwords, apply security updates, etc. Manufacturers can build the strongest capabilities into a device or service, but the likelihood that device or service is compromised by a cyber-attacks increases if end-users or operators do not undertake appropriate precautions.

Ensure the Labeling Format is Flexible and the Content is Effective

- A cybersecurity "label" should not only be conceived of as a physical sticker, especially in the digital space. The 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.

- An e-label is a digital representation or an electronic means to display regulatory and other important information. E-labeling can often be achieved by using a product or services' own built-in display, providing links to an internet website, or providing a scannable source. E-labeling 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.

- For communication to be effective for end-users, any cybersecurity labeling scheme should streamline and simplify necessary information for the intended audience. This should include avoiding unnecessary information that may distract end-users from understanding important security considerations. The depth, complexity, and comprehensiveness of security information in a label should be reflective of the end-user to whom the label is intended to inform. Some sophisticated end-users and operators may need detailed security information, but lay end-users may find such detail unhelpful.

- We recommend governments engage stakeholders to determine the most effective set of information that should be included in security labeling communications. what information is appropriate may differ depending on the type of product and intended audience (i.e., industrial technology for enterprise versus IoT devices for individual consumers). Policymakers may consider whether it makes sense to include discrete types of information such as related certification, date of issue, name and contact information of the manufacturer, the functionality, and the security features, though ITI recommends maintaining the maximum amount of flexibility in this regard. Colors, national flags, or unique designs are not necessary information to convey security. Instead, they might lead to unhelpful market access issues or trade barriers.

- 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, which would discourage adoption. We recommend that policymakers consider conducting periodic reviews to assess the usefulness, effectiveness, and cost of cybersecurity labeling, as well as the impact of the labeling on improving security and end-users' decisions. Such assessments can help policymakers progress toward policy objectives, make needed adjustments, and better direct resources.

- ITI encourages labeling and related certification to be voluntary and to only consider requiring labels and conducting related enforcement if policymaker evaluations of labeling and related certification programs determine that they are necessary in particular circumstances.
- In such circumstances where it is determined that labels must be required, ITI encourages enforcement authorities to conduct fair enforcement and ensure there is clear, efficient, harmonized regulatory enforcement and guidance across jurisdictions to help accelerate industry adoption, including appropriate market surveillance and proportionate penalties.

Ensure Labeling Does Not Convey a False Sense of Security

- A label should not indicate that a product is completely secure. Such an assumption would create a false sense of security and can serve to undercut the necessity for 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.
- Cybersecurity is a continuous process of protecting ICT products and services, as well as the networks and complex ecosystems of which they are a part, based on the latest threat/vulnerability information. Policymakers should recognize that a label only reflects a set of cybersecurity features or processes at a specific point in time. In some cases labeling might provide a useful way to communicate information about cybersecurity, but due to the dynamic and constantly evolving nature of cyber threats, the long period of time and effort it takes to adopt a labeling scheme in many cases means that a labeled product or service may no longer reflect leading-edge security practices and may not account for the latest innovations.
- If possible, companies should have the option to decide whether to link the physical or electronic cybersecurity label to reflect organizational lifecycle security processes to a website, such as secure development, vulnerability scanning, regular security updates, and further security documentation above and beyond the minimum requirements where possible. Doing so will help to further communicate to end-users how a vendor develops its products and services, which is often a more appropriate indicator of security than a point-in-time approach.

Align with International Standards and Focus on Features

- ITI supports voluntary cybersecurity labeling for finished consumer products as a general matter in certain verticals (e.g., consumer IoT) where a clear benefit is established (e.g., increasing end-user awareness). However, in more sophisticated verticals (e.g., enterprise), where end-users do not have the same "information asymmetry" problem as exists between manufacturers and consumers, even voluntary labels may provide no discernible benefit.
- Cybersecurity labeling schemes should be grounded in international, industry-led, voluntary consensus standards and frameworks, and designed in a manner that meets the needs, risk postures, and policy objectives of the relevant sector or manufacturer. ITI supports adoption of security baselines consistent with

international standards and best practices and encourages governments to consider which baseline requirements may be appropriate to incorporate into labeling criteria to facilitate consistency and effectiveness.

- Requiring unique, specialized, or local features disconnected from fundamental security practices may create trade barriers, subject end-users to unnecessary or confusing information, and potentially burden companies by causing a fragmented approach to security labeling for different jurisdictions. We encourage policymakers to facilitate the mutual recognition of labeling across jurisdictions, as well as third-party assessment labs. Doing so will help ensure prioritization of international standards-based programs, thus reducing fragmentation.
- Where applicable, the related certification requirements for attaining the label should indicate the product or service's conformance to a specific international standard or to widely accepted best practices where the requirements are broadly applicable to the relevant sector, can be assessed to tangible, attestable, practical criteria and not aspirational guidance.

ITI

Promoting Innovation Worldwide

www.itic.org