Report for the Assistant to the President for National Security Affairs (APNSA) on Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software

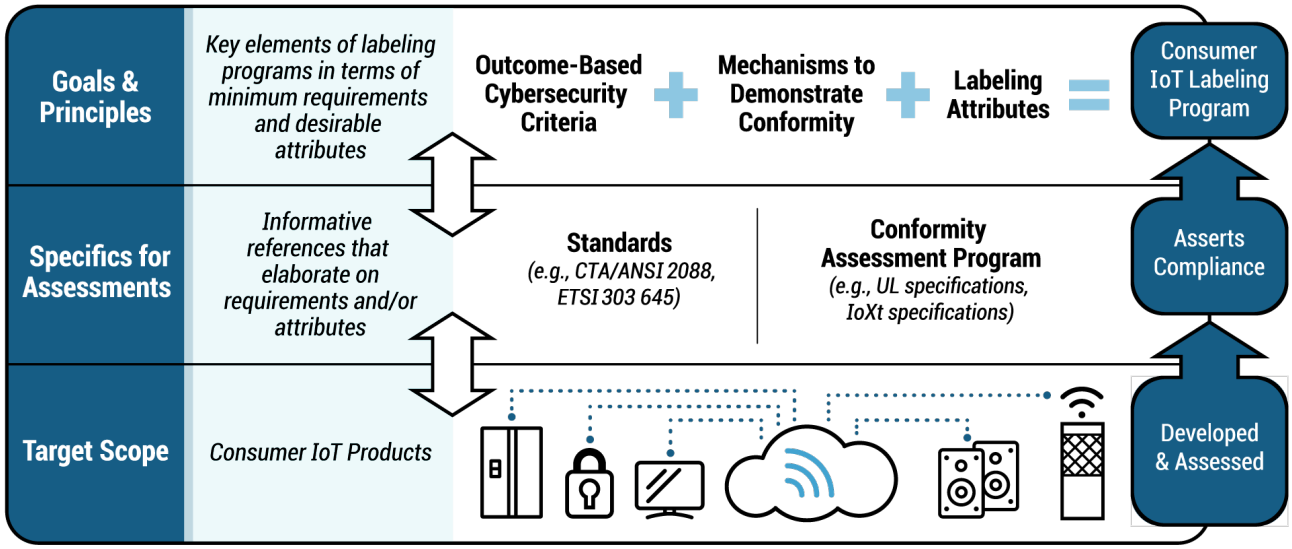
A summary review of labeling actions called for by Executive Order (EO) 14028: Improving the Nation's Cybersecurity

May 10, 2022

1. Overview

Executive Order (EO) 14028: Improving the Nation's Cybersecurity (May 12, 2021) assigned actions to various federal agencies. Section 4 of the EO instructed NIST to take a variety of steps, including initiating cybersecurity labeling pilot programs in two areas: 1) consumer IoT devices and 2) consumer software development practices. Based on robust private and public sector stakeholder engagement (see Section 2), NIST identified recommended criteria for cybersecurity consumer labeling for IoT products and consumer software development practices (see Section 3). Following the publication of the recommended criteria, NIST initiated a pilot, soliciting contributions about participation in potential labeling programs (see Section 4).

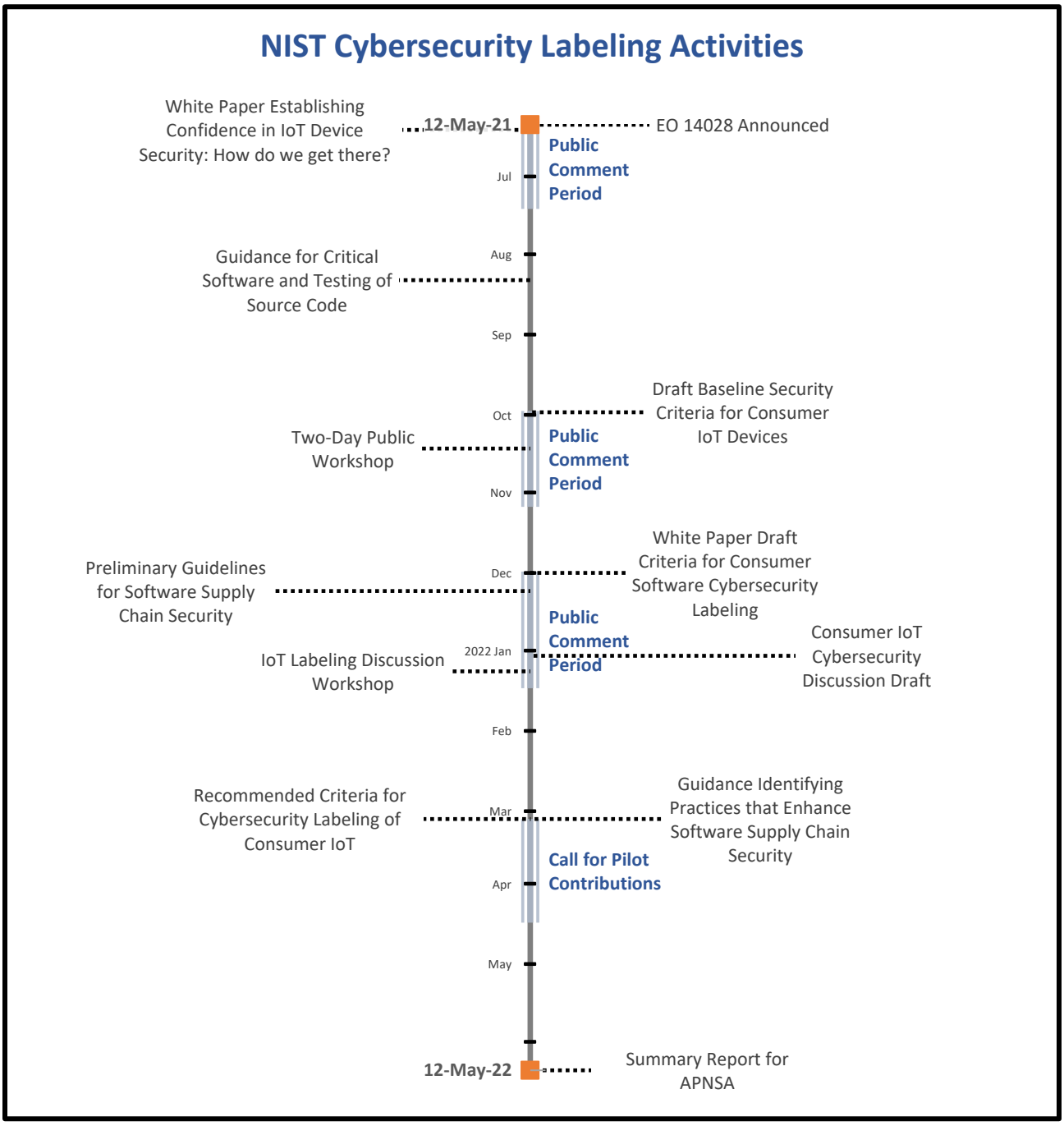
Within one year of the May 12, 2021, EO, NIST was instructed to review, in consultation with the private sector and relevant agencies, the effectiveness of the pilot programs and to determine what improvements can be made. This document summarizes that review.



2. Stakeholder Engagement and Feedback

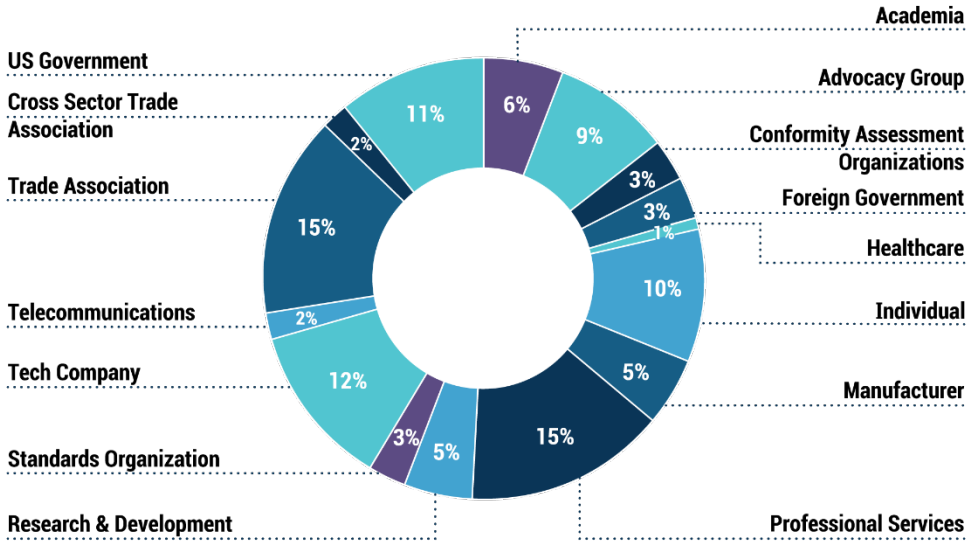
NIST gathered a broad range of input from experts in industry, academia, and civil society as well as the public sector broadly in carrying out the EO's provisions related to consumer cybersecurity labeling. NIST coordinated with the Federal Trade Commission (FTC), which also contributed to the first NIST workshop and facilitated several meetings with stakeholder groups. Furthermore, NIST coordinated with other federal agencies, including the Environmental Protection Agency (EPA) and the Consumer Product Safety Commission (CPSC) as well as with the Interagency Committee on Standards Policy (ICSP) and the federally chartered Cybersecurity Solarium Commission.

Throughout the process of developing criteria and labeling program approaches, NIST held listening sessions with private sector stakeholders, including industry associations, consumer representatives, companies, and standards and conformity assessment bodies.



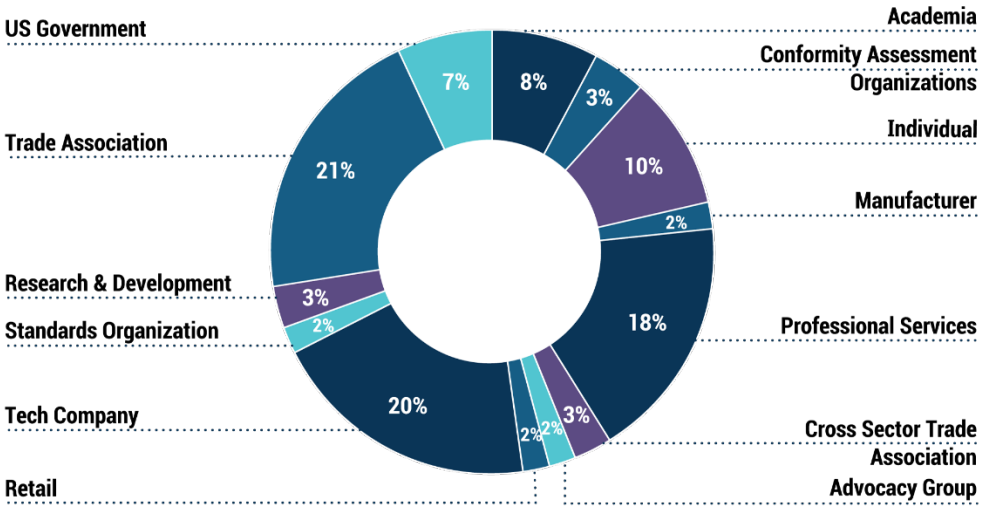
NIST received responses from 102 commenters on the consumer IoT labeling criteria and 61 commenters on the consumer software labeling criteria. The charts below provide an overview of the range of stakeholders providing input to the respective cybersecurity labeling efforts.

NIST received responses from 102 commenters on the consumer IoT labeling criteria.



Response Representation for EO Consumer IoT Labeling Criteria

NIST received responses from 61 commenters on the consumer software labeling criteria.



Response Representation for EO Consumer Software Labeling Criteria

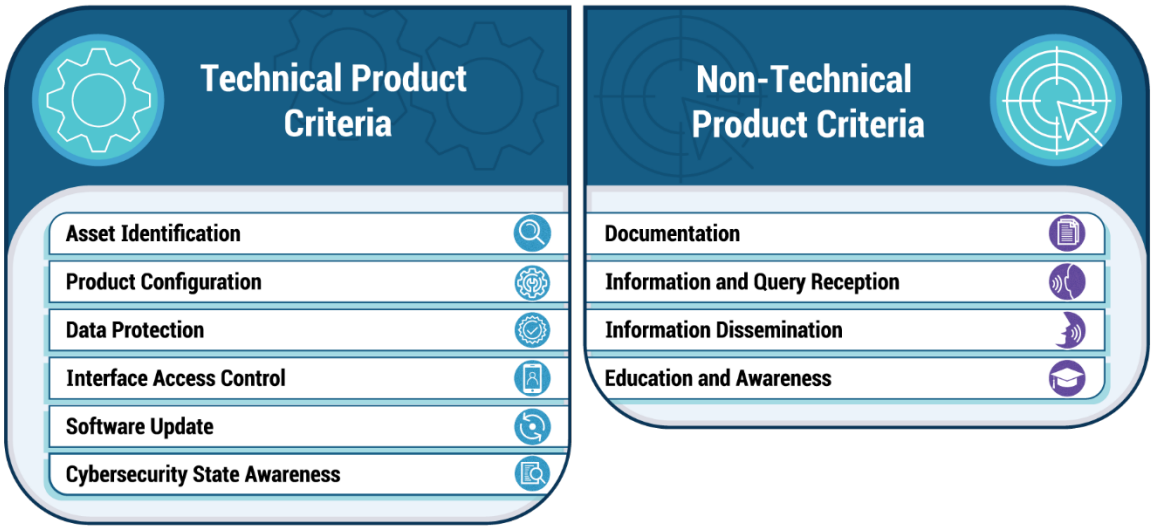
3. Arriving at the Recommended Criteria

The NIST draft IoT product criteria and consumer software criteria received strong support. In February 2022, NIST published Recommended Criteria for Cybersecurity Labeling of Consumer Internet of Things (IoT) Products and Recommended Criteria for Cybersecurity Labeling of Consumer Software. These final recommended criteria each included three critical elements to consumer cybersecurity labeling: the criteria (what manufacturers or software developers do to address cybersecurity); the label (how cybersecurity information is communicated to the consumer); and conformity assessment (demonstration that the criteria were met).

Each element is presented followed by discussion of the themes from stakeholder feedback received around that topic that were critical to the development of the recommendations.

Cybersecurity Criteria for Consumer IoT Products

The final form of the cybersecurity criteria for consumer IoT products is displayed below, followed by an overview of the common themes from stakeholder feedback.



Baseline IoT Product Criteria

Common themes from stakeholders:

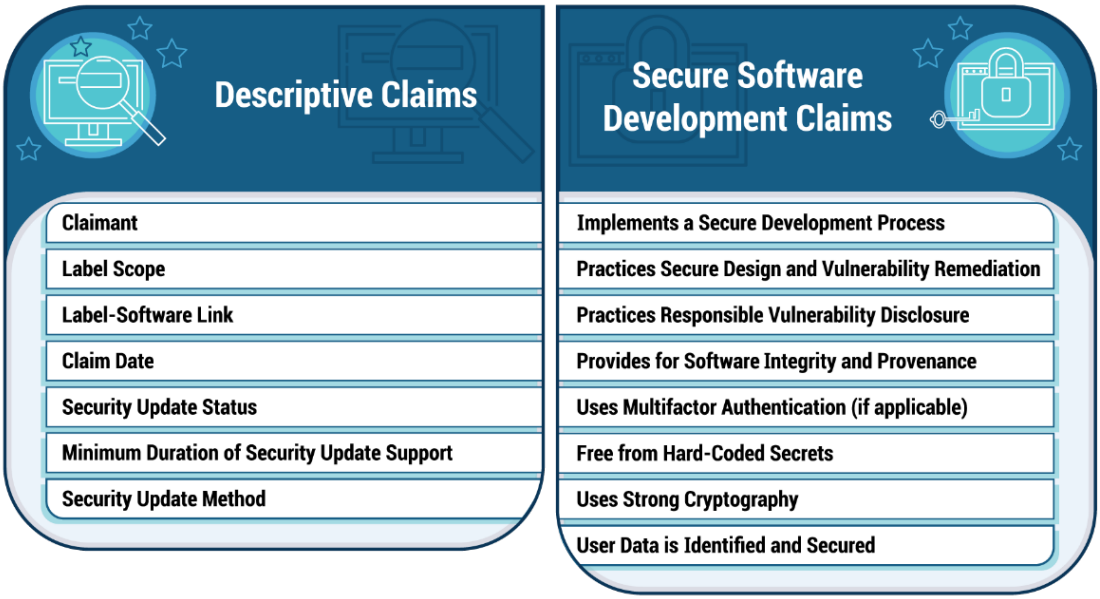
- Adapting existing NIST non-sector-specific IoT cybersecurity guidance to consumer products was encouraged as a starting point for determining NIST's recommendations for the consumer IoT product cybersecurity criteria.
- Focusing on cybersecurity *outcomes* received strong support. The outcome-based approach and flexibility enable adoption of the appropriate standards and allow standards to evolve and meet the need of a wide variety of devices. This approach helps address the variety of IoT products used by consumers.
- Scoping the IoT product criteria to include all components of the IoT product (and not just the device in the 'box') was encouraged – and highlighted potential challenges for scheme owners, taking into account that IoT product components have different sources, architectures, maturity, and risks.
- Some feedback encouraged considering whether a label would cover the potential privacy impact of the IoT product and the implementation of the cybersecurity criteria. While some aspects of privacy, such as

confidentiality of data, are cybersecurity objectives, NIST recognizes that other aspects of privacy are not covered by the cybersecurity criteria – such as problematic data actions (the likelihood of any given problem arising from data processing).

- Using tiers without consideration for contextual risk that depends on the product use was deemed of limited value. Feedback indicated that no specific criteria outcome could be excluded in developing tiers without further information about the IoT product and use case for that product. It was unclear whether the consumer will be expected to make that risk determination based on product characteristics or whether an authoritative source would do this. Guidelines to assess the risk of IoT products were considered to be limited.

Cybersecurity Criteria for Consumer Software

The final form of the cybersecurity criteria for consumer software is displayed below, followed by an overview of the common themes from stakeholder feedback.



Consumer Software Technical Baseline Criteria

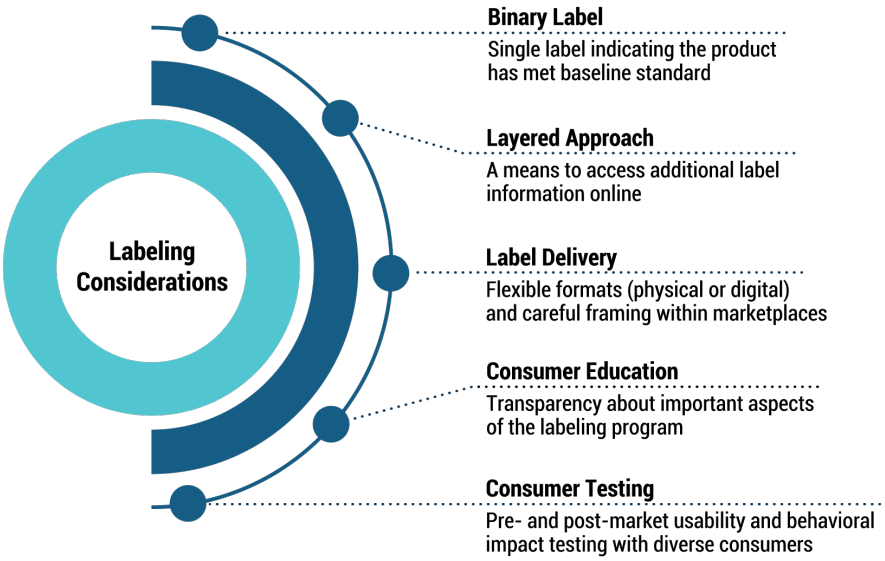
Common themes from stakeholders:

- There was strong support for including NIST's Secure Software Development Framework (SSDF) in the criteria, noting that the framework itself is intended to capture and include what is already considered industry best practice.
- Some concern was expressed over the lack of privacy criteria.
- Challenges were cited with end-of-life/expiration dates for software. Feedback was consistent that a label should convey to the consumer if, and for how long, a piece of software would receive security-related updates. However, industry stressed that making such claims could negatively influence industry participation due to liability concerns. NIST addressed those potentially conflicting views by including criteria that allowed consumers to make informed decisions regarding longevity of software *and* permitted manufacturers flexibility in making support claims.

- Stakeholders emphasized the need to craft labeling criteria to avoid lulling consumers into a false sense of security. Strong development practices and reasonable product criteria can help to minimize both the occurrence and the impact of cybersecurity failings. However, making such a claim via a label does not necessarily mean any one product *is secure* or is *more secure* than any other. Similarly, the lack of known product vulnerabilities does not assure that a product is vulnerability free. Labeling criteria should not engender these misinterpretations.

Development of the Label

The same considerations apply to the creation of the label for IoT products and consumer software. The figure below depicts the labeling considerations established in parallel with the technical criteria development.



Common themes from stakeholders:

- Stakeholders noted that the usability of the label and consumer education materials is important to ensure accessibility to diverse consumers with differing backgrounds and abilities. Others noted the difficulty in conveying complex cybersecurity information to support consumer decisions and avoid misconceptions.
- There was a desire for multiple stakeholders to share responsibility for consumer education and testing rather than those being the sole responsibility of the scheme owner.
- Stakeholders expressed the need for the label to be flexible to reflect changing security and label status and that label information be easily accessed before, during, and after product selection.
- Stakeholders also noted the importance of engaging retailers and product marketplaces in label delivery, as these entities are often the first point of consumer contact.

Conformity Assessment

Common themes from stakeholders:

- Viewpoints on conformity assessment approaches were mixed. Some stated preference for self-declaration, while others supported third-party assessment. For consumer software, the preferences related to the software development process and/or software itself. While the outcome-based approach

taken for the labeling efforts received positive feedback, some stakeholders highlighted the potential risks of market fragmentation that could result from the flexibility offered in conformity assessment.

- The existence of multiple scheme owners and the potential for more schemes to be introduced create a need for further definition of scheme owner characteristics, such as role and scope of responsibilities and cost to scheme owners of incentive programs. Comments also identified the need for an entity to evaluate scheme owner(s) themselves to ensure consistency of requirements across schemes.

4. Cybersecurity Labeling Pilots

The EO directed NIST to conduct and review pilots, consult with the private sector and relevant agencies to determine what improvements can be made, and then submit a summary report.

In the pilot, NIST sought contributions from stakeholders about current or potential future labeling efforts for consumer IoT products and consumer software and about the alignment of those efforts with the NIST recommendations.

NIST did not design a particular label – nor did NIST establish its own labeling program for consumer software or consumer IoT products. Rather, the recommended criteria specified desired outcomes, allowing providers and customers to choose the best solutions for their devices and environments. NIST recognized that one size will not fit all, and multiple solutions might be offered by label providers.

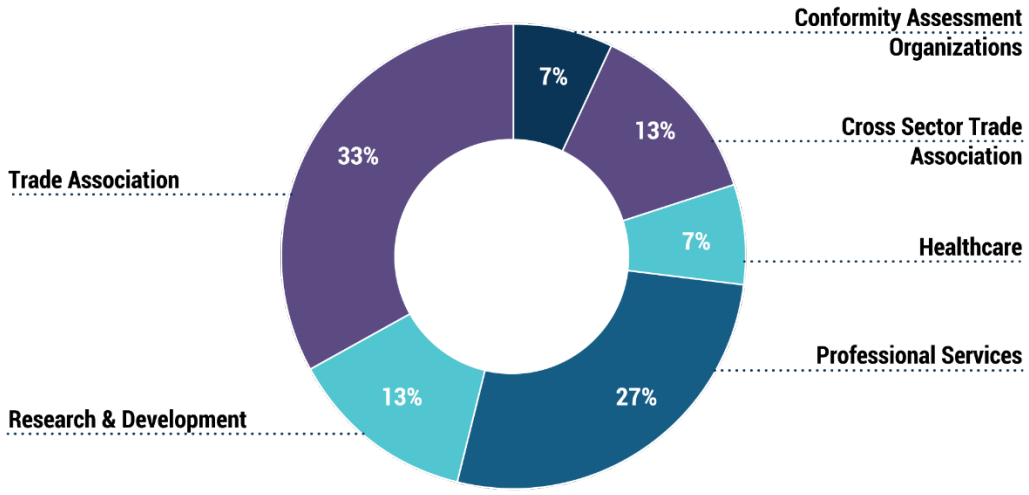
NIST requested contributions on any of the following issues during the pilot:

- Whether there are existing labeling schemes that partially or completely align with the NIST recommendations, including information regarding that alignment;
- Whether organizations that do not currently operate labeling schemes would be interested in establishing new programs based on the NIST recommendations;
- The type of organization(s) that could serve as owner(s) for consumer labeling schemes;
- Recommendations on how a scheme owner would utilize the NIST recommendations to manage a labeling program; and
- Potential incentives for implementing a consumer labeling scheme based on the NIST recommendations.

NIST received 17 written responses from organizations that could perform a range of roles within a labeling scheme:

- Scheme owner
- Owner of a specification or standard that maps to some or all the recommended criteria (note that these mappings were very detailed using NIST's National Online Informative References (OLIR) template)
- Conformity assessment body
- Supplier of other support services for the labeling scheme

Multiple organizations offered to serve in each of the different roles. Because the pilot phase focused on gaining information from potential providers in a labeling scheme, written responses were primarily from organizations that could perform these roles:



Response Representation for Pilot Feedback

Throughout the pilot process, NIST held sessions with private-sector stakeholders, including industry associations, professional services organizations, research and development firms, and conformity assessment organizations. In addition to support for the recommended criteria for consumer IoT products and consumer software, organizations expressed interest in becoming a scheme owner. Major feedback included the following:

- A significant majority of the contributions focused on the IoT product criteria due to the level of international activity in establishing mechanisms, especially labeling schemes, to improve IoT cybersecurity. While cybersecurity for traditional software and IT products is a technical field with a far longer, more established history, labeling for cybersecurity has not been as widely considered.
- Industry was supportive of NIST continuing to maintain and evolve the criteria over time using its regular processes for stakeholder input.
- Virtually all stakeholders recognized the critical importance of scheme owners to the success of consumer labeling efforts. Stakeholders stressed that coordination across schemes would be needed to ensure consistency across sectors and product types.
- Those providing input cited the need for private-sector and government participation in international standards development to encourage alignment and harmonization across efforts.
- Manufacturers, software developers, retailers, and others that participate in future labeling efforts would likely be taking on liability, even if these programs are voluntary. Those liability challenges were said to include having labels misconstrued as warranties and label statements misattributed as endorsements by digital storefronts and retailers. Moreover, stakeholders posited that without adequate legislative/regulatory protections, participation in labeling programs would likely suffer, despite being voluntary.
- Many of the organizations expressing interest in participating in IoT product or consumer software labeling identified existing or future labeling programs or declarations of interest. Several submitted OLIR mappings of existing standards.
- A few organizations with ongoing IoT conformity assessment programs demonstrated alignment with the recommended criteria in a variety of ways.
- Several stakeholders provided feedback related to development of the label and consumer education materials. They provided examples for how to link the physical label to additional online product-specific information and discussed the alignment of the binary label to outcome-based criteria. They also

emphasized the importance of consumer education materials to facilitate understanding of the labeling scheme and provided input on who (for example, manufacturer or scheme owner) would host the online label and consumer education materials.

5. Conclusions

Results from the pilot showed clear interest in consumer cybersecurity labeling programs for IoT products and software. At the same time, there was a recognition of many challenges involved in launching and managing such programs in a complex and dynamic landscape. Robust stakeholder engagements made clear that if such labeling programs are to succeed, important steps would need to be taken to support their final development and provide incentives for establishment and implementation – with industry and government each playing important roles.

The feedback NIST received repeatedly highlighted the following considerations for industry and government – informed by consumer interests – that are essential to incorporate in implementing a strategy for a consumer cybersecurity labeling program:

- **A consistent label design is critical to reduce consumer confusion, build label recognition, and increase consumer demand for labeled products**. Ensuring label consistency regardless of which organizations manage a labeling scheme is key, especially if consumer cybersecurity labeling efforts will involve multiple scheme owners. In addition, any label design should have thorough pre- and post-market testing. Associated consumer education materials will be required to ensure the label will be accepted and understood by all stakeholders (e.g., different kinds of consumers, retailers, developers).
- Consumer awareness is critical to build market demand. However, **the scale of efforts to educate the public on the cybersecurity label should not be underestimated and will require a large investment of resources** (e.g., financial and time). NIST heard that government support would be needed.
- Stakeholders also noted that consumer IoT products and software are not used in a vacuum and cybersecurity related to these products depends on more than what can be tested for or communicated via a label on the product. Therefore, **consumer awareness and education about cybersecurity labeling efforts need to be part of a broader initiative to equip consumers to address cybersecurity issues.** This will be a significant, long-term investment requiring the participation of multiple stakeholders across both the public and private sectors.
- An approach that focuses on defining the desired cybersecurity outcomes to be achieved by the product **must provide the flexibility to encompass the wide range of product capabilities and configurations.**
- NIST heard that **multiple scheme owners may be necessary** to ensure that a consumer IoT product labeling effort can adequately cover the variety of products available today and to be offered in the future.
- Ensuring consistent and quality assessments of outcomes likely will necessitate the involvement of a **third-party authority responsible for coordinating across scheme owners and other key stakeholders.** Possible responsibilities for this authority include evaluating how outcomes are addressed by each scheme and what standards and conformity assessment activities are adopted.
- **The liability of key stakeholders throughout the ecosystem may discourage the voluntary adoption of a cybersecurity label.** Liability protections for scheme owners and other scheme participants must be addressed by government**,** perhaps through legislative or regulatory actions.
- A common set of **outcome-based cybersecurity criteria that underpin the label should be maintained and updated over time** for a cybersecurity labeling effort. Technologies, risks, and mitigations will

change in ways that will need to be reflected in the criteria. The criteria also will need to take into account new information as they are adopted and used. Feedback indicated that NIST should continue to work with stakeholders to maintain and update the IoT product criteria in the near term to help ensure their consistency and reliability.

- **There is a need for a robust marketplace of standards that industry can put into practice and scheme owner(s) can employ to consistently assess products to be labeled.** This will require active industry and federal government participation in international standards efforts, which also will encourage international alignment and harmonization.
- Considering the great interest internationally and across multiple economies to implement label and certification schemes, **there was strong support for mutual recognition of schemes between national economies** to reduce the burden on manufacturers**.** Some stakeholders identified a need for a US government role to enable such recognition across national economies.