

15 March 2022

National Institute of Science and Technology
Labeling Executive Order

Ref: NIST “Consumer Cybersecurity Labeling Pilots: The Approach and Contributions”

Dear NIST Labeling Executive Order staff,

The TIC Council Americas is pleased to provide comment on “Consumer Cybersecurity Labeling Pilots: The Approach and Contributions” and NIST Recommended Criteria for Cybersecurity Labeling of Consumer IoT Products and Recommended Criteria for Cybersecurity Labeling of Consumer Software.

We and our members support all efforts to address cybersecurity in connected infrastructure¹, systems, components, devices and software and look forward to our ongoing engagement and discussion on this topic.

We agree that one size may not fit all, and that multiple solutions might be offered by label providers to support consumers in better understanding the cybersecurity function and level of cybersecurity offered by the products or software they chose to purchase. However, we would add that conformity assessment and specifically testing, inspection, and certification, are critical in assuring that the products and software produced or operated have the required characteristics, and that these characteristics are consistent from product to product or software to software. “While each of the conformity assessment activities are operated independently, they are closely interrelated. The inclusion or absence of any of these activities, as well as the competence, consistency and impartiality with which any one of them is performed, can have a significant effect on the confidence and reliance that can be placed on the results of the entire conformity assessment process.”

As explained in NIST Special Publication 2000-01, ABC’s of Conformity Assessment, A Supplier Declaration of Conformity (e.g., SDOC) is used when the risk – to consumers, users, and others – is low and there are suitable safeguards such as penalties in place and/or mechanisms to remove the products from the market.

When examining the use case of IoT functional devices and software, the risk to consumers, users, and others is high. These products and software do not exist in the absence of other products and software. As explained in the NIST guidances, these products and pieces of software are designed to share information with, to gain information from, and in some cases work in unison with other products and software creating an ecosystem where the risk may affect whole communities of parties separate from the one individual who made the purchase.

Due to this, a product or software that lacks appropriate cybersecure mechanisms places us all at direct risk to cyber intrusion, theft of real and intellectual property, and potential physical harm. These devices and software may not be easily removed from the market or updated in time to prevent the significant harm they would cause.

¹ https://www.tic-council.org/application/files/5915/5775/4670/IFIA_One_Pager_IoT_and_Cybersecurity.pdf

By creating an environment where a label is the norm, without establishing a clear oversight mechanism to police that environment, will lead to the use of labels to gain access to the market without a clear commitment and testing, inspection and certification data to support the information and potential claims included on those labels. Who approves a product to have a label? Who vets that a product meets labeling requirements? And what enforcement is available if a label provides misinformation? We recognize through participation in NIST workshops and speaking with human factors experts that consumers will trust the labels on these products and in many cases, will not have technical support or expertise to evaluate whether the claim made is genuine. For these reasons, the use of independent third-party conformity assessment as a required step in any labeling scheme must be a requirement and not a recommendation.

Using a combination of cybersecurity standards, evaluation, and independent third-party certification will support industry and scheme owners in addressing systems security and risk management. Conformity assessment is a reasonable and responsible model for addressing the challenges of acquisition and cybersecurity and improving cybersecurity posture throughout software and product lifecycles. And trusted, independent third-party conformity assessment is a cost-effective policy solution as it provides the highest level of confidence and helps leverage private-sector resources.

A third-party certification body is defined as acting independently and therefore, without bias and consumers should be clearly informed of this difference in impartiality and any and all labeling schemes should reflect and communicate this distinction.

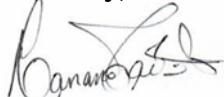
The TIC Council Americas looks forward to working with agencies, consumers, and industry stakeholders in the development of conformity assessment labeling schemes for the cybersecurity of products and/or software to support the establishment of a robust conformity assessment program which incorporates independent third-party testing, inspection, and certification.

Please see attached the TIC Council Americas' responses to NIST questions regarding TIC Council Member labeling schemes.

TIC Council is a global association representing over 90 international independent third-party testing, inspection, certification and verification organizations. Testing, Inspection and Certification (TIC) companies cater to a diverse range of industry sectors and a variety of standards and legislation. The industry represents an estimated one million employees across the world with annual sales of approximately USD 200 billion.

We appreciate the opportunity to give feedback on "Consumer Cybersecurity Labeling Pilots: The Approach and Contributions" and NIST Recommended Criteria for Cybersecurity Labeling of Consumer IoT Products and Recommended Criteria for Cybersecurity Labeling of Consumer Software. Should you have any questions, please don't hesitate to contact Karin Athanas at +1 240 762 8069 / kathanas@tic-council.org.

Sincerely,



Hanane Taidi
Director General
TIC Council



Karin Athanas
Executive Director
TIC Council Americas
kathanas@tic-council.org

Question Responses

Whether there are existing labeling schemes that partially or completely align with the NIST recommendations, including information regarding that alignment.

Response:

There are numerous cyber labeling programs available to industry offered by members of the TIC Council. These programs, offered by third-party conformity assessment bodies, provide trust to consumers through their impartial review of software and product functionality with cybersecurity requirements.

They help to educate consumers to the level of cybersecurity or elements of cybersecurity features offered by the software or product and serve as an independent verifier of claims by manufacturers and software companies.

The TIC Council has notified its members of the need to compare their programs with the NIST recommended guidance and they will be submitting additional feedback separately as to how closely their programs align with the NIST recommendations.

We would, however, also note that claims by manufacturers continue to be prevalent. In one such case, a contractor failed to alert a customer to potential failures in cybersecurity compliance.² Unclear declarations by manufacturers could potentially create confusion in the market. The Department of Justice in October 2021 launched the Civil Cyber-Fraud Initiative to “combat new and emerging cyber threats to the security of sensitive information and critical systems.” In their announcement the Department states that “The initiative will hold accountable entities or individuals that put U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services,” a growing concern for the agency.³

Without clear benchmarks and oversight of cybersecurity labeling schemes, the number of programs available will only grow and an unchecked system will lead to false claims, confusion, and a loss of confidence in labeling by consumers.

Whether organizations that do not currently operate labeling schemes would be interested in establishing new programs based on the NIST recommendations.

Response:

As previously noted, the members of the TIC Council currently offer labeling schemes, and many may also be developing new labeling schemes to meet the needs of this quickly changing and innovating industry. However, it is important to note that in an environment where a cybersecurity label is expected, manufacturers and software developers will develop their own programs to gain access to the market.

This will lead to an unchecked system where a lack of consistency between labels will create confusion and distrust and as a result, the label will fail to have true value for consumers.

² See United States ex rel. Markus v. Aerojet RocketDyne Holdings, Inc., related news: <https://www.jdsupra.com/legalnews/incomplete-cybersecurity-compliance-9417141/>

³ Department of Justice, “Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative,” <https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative>

To address this, we recommend that a mechanism to police the use of labeling be established.

The type of organization(s) that could serve as owner(s) for consumer labeling schemes.

Response:

In the view of the TIC Council Americas, any organization wishing to manage, oversee, or own a consumer labeling scheme should ensure the scheme requires the use of independent third-party conformity assessment providers and be open, available, cost-conscious, and does not create undue burdens on the participation of the independent third-party conformity assessment industry.

The oversight of cybersecurity labeling schemes, due to significant risk to consumers, would benefit from the involvement of a government agency serving in the oversight role. This would not eliminate or preclude organizations from developing a labeling scheme, but would create the necessary oversight for those schemes, the conformity assessment supporting them, and the information shared with consumers through labels to be evaluated.

For government agencies that might consider overseeing such a program, the TIC Council America would recommend programs such as Energy Star or OSHA NRTL as effective programs that could be used as a template. Trusted independent third-party conformity assessment is a cost-effective policy solution as it provides the highest level of confidence and helps government leverage private-sector resources.

Oversight by industry, while common and a 'best-fit' in many cases, is not recommended due to the risk associated with cybersecurity failures and the high level of technical complexity associated with software and product design and the evolving nature of cybersecurity threats. Third-party TIC providers are highly trained in thousands of standards, rules, and regulations and in their application to a wide range of products and software. This makes them uniquely qualified to evaluate emerging and innovative products not yet encountered on the market.

Through partnership between an oversight government agency and the independent third-party TIC Industry and mirroring a program such as Energy Star or OSHA NRTL, an effective, cost-conscious, and consumer-oriented program could be developed.

Recommendations on how a scheme owner would utilize the NIST recommendations to manage a labeling program.

Response:

A government agency(ies), through use of the NIST National Framework for Improving Critical Infrastructure Cybersecurity and a broad range of published consensus-based standards, could establish in partnership with the independent third-party TIC Industry, a program which mirrors the approach used in the Energy Star or OSHA NRTL programs. These programs have been found to be effective, cost-conscious, and consumer-oriented to support the development of compliant products which communicate effectively to consumers the safety, functionality, and reliability of those products.

Potential incentives for implementing a consumer labeling scheme based on the NIST recommendations.

Response:

A government agency(ies), through use of the NIST National Framework for Improving Critical Infrastructure Cybersecurity and a broad range of published consensus-based standards, could establish in partnership with the independent third-party TIC Industry, a program which mirrors the approach used in the Energy Star or OSHA NRTL programs.

Such programs have many benefits and if applied to consumer labeling, could provide:

1. Improved trust among consumers
2. Decreased cyber incidents
3. Reductions in cost for manufacturers and retailers related to legal actions by consumers and industry customers
4. Reductions in time-to-market through a consistent and reliable product and software review process
5. Improvements in response time from identification of a cyber threat to updates, recalls, and corrections communicated to software and product users
6. Establishment of a clear recall or product update process, ensuring products that don't meet cybersecurity requirements, are unsafe, or insecure, are quickly updated or removed from use.
7. A clearer view of the chain of responsibility within the supply chain.