Before the

National Institute of Standards and Technology

U.S. Department of Commerce

COMMENTS OF THE ANSI NATIONAL ACCREDITATION BOARD REGARDING

DRAFT BASELINE CRITERIA FOR CONSUMER SOFTWARE CYBERSECURITY LABELING

1. Introduction and Statement of Interest

The ANSI National Accreditation Board (ANAB) hereby submits its comments in response to the National Institute of Standards and Technology (NIST) request for comments on the "Draft Baseline Criteria for Consumer Software Cybersecurity Labeling" document.[1]

The ANSI National Accreditation Board (ANAB) is the largest multi-disciplinary accreditation body in the western hemisphere, with more than 2,500 organizations accredited in approximately 80 countries. A non-profit and wholly owned subsidiary of the American National Standards Institute (ANSI), ANAB has comprehensive signatory status across multilateral recognition arrangements of the International Accreditation Forum (IAF) and International Laboratory Accreditation Cooperation (ILAC). ANAB helps industry and facilitates trade by providing accreditation and training and serving as architects for the conformity assessment structure of industry-specific programs.[2]

[1] *See:* NIST Consumer Software Criteria and the Draft Baseline Criteria for Consumer Software Cybersecurity Labeling document was developed by NIST in response to the assignment given under the Presidential Executive Order on Improving the Nation's Cybersecurity (14028) issued on May 12, 2021. NIST is seeking comments on the draft criteria, which suggests a set of potential baseline security criteria for consumer software.

[2] *See:* https://anab.ansi.org/

2. Comments

ANAB submits the following comments, relating in particular to the questions included in the "Draft Baseline Criteria for Consumer Software Cybersecurity Labeling" document.

a) *Whether criteria will achieve the goals of the EO by increasing consumer awareness and information and will help to improve the cybersecurity of software which they purchase and use.*

   ANAB agrees that the criteria will help achieve the goals of the executive order. It will be important to have consumer education activities as stated in the document in order to make the consumers aware of benefits of the program.

b) *Whether the criteria will enable and encourage software providers to improve the cybersecurity aspects of their products and the information they make available to consumers.*

   ANAB agrees that the criteria will encourage software providers to improve the cybersecurity aspects of their products. It is expected that by completing the exercise of demonstrating compliance it will motivate software providers to take steps to improve the cybersecurity aspects of their products.

   In order for the criteria to motivate meaningful change, it may be beneficial to leverage third-party review for some of the attestations, in order to validate that the attestation is correct and meaningful. For example: vulnerability reporting is so critical to the safety and security of consumers that third-party review of vulnerability methodologies and confirmation of results as stated in the attestations may help increase the trust and assurance that the consumer has in the label. As such it may be beneficial to have the vulnerability reporting attestation objectively confirmed by a third-party and stated in the SDoC.

c) *Whether the labeling-specific criteria are appropriate and likely to be effective for consumers.*

The labeling-specific criteria are comprehensive and well considered. The analysis provided in the appendix outlining the rationale behind a binary, layered approach is compelling.

d) *Whether a single, overarching statement that the software product meets the NIST baseline technical criteria should be included on a label, or whether alternative statements would be appropriate.*

ANAB agrees that a single overarching statement should be included on the label. A simple label will generally be most effective in communicating with the consumer. Using the layered approach as described in the appendix is optimal, where additional information on the program can be provided via a reference to a website that is included in a binary or otherwise simple label.

e) *Whether additional considerations for the labeling approach, consumer education, or testing are needed – including:*

- *Possible appropriate definitive text for describing the labeling program in consumer education materials*
- *Best approaches for addressing the needs of non-English speaking consumers*

Additional information should be supplied as part of the pilot program to aid in the consumer education effort. Consumers benefit from being notified of these labels, as well as where to obtain information about the criteria represented by the label. The label could also include branding or linkage to the eventual scheme owner, where definitions and details on the meaning of the label can be elaborated.

Use of icons may be beneficial to convey meaning to non-English consumers, if coupled with a reference or mechanism to look up the definitions of each icon online in multiple languages.

f) Whether the software label approach and design should be unique or extended to the IoT product label (also directed in the EO) to facilitate brand recognition, even though the technical criteria will be different.

The software label approach and design should be extended to the IoT product label to help avoid confusion in the marketplace. It is anticipated that the consumer will not understand the difference if more than one label is used. This will also aid in educating the consumer on what label and related information they should be looking for.

g) Whether the conformity assessment provisions are appropriate.

Scheme Owner. Include information on how NIST will interact with potential scheme owners of the pilot program. Provide guidance on how the program will operate if there is not a scheme owner and is based solely on use of a SDoC. Recommend that a discussion on the scheme owner responsibilities be included in the draft document to help clarify the intention of how the program will be administered.

Once the program is finalized, it is recommended that the body responsible for the ongoing maintenance of the scheme be identified. There is a need to identify how recommendations for revisions to the program will be considered.

Provide information on what elements should be in the scheme. For example, consider the following:

- Registration. In order to provide supporting information on the implementation of the pilot programs for cybersecurity labeling, it is recommended that a record (database) of each SDoC be maintained by the scheme owner. This will aid in the surveillance and review of the effectiveness of the pilot program. A record of each SDoC issued will allow NIST to evaluate to what extent that the pilot program is being used.
- Attestation Validation: In order for the SDoC to be meaningful, there should be third-party evaluation of key elements of the attestation for appropriateness of selected security practices and the correctness of implementation. While the impact of mandatory use of an accredited laboratory or inspection body could result in considerable burden to the software developer, the consequences of optional self-attestation may result in a lack of trust in the label. To mitigate this risk, it may be beneficial to require random or periodic inspection of their conformity assessment methodology by an impartial third-party.
- Surveillance. In order for the SDoC to be effective there needs to be a surveillance activity to determine if the software is correctly labeled in accordance with the requirements of the program.

- Complaints. Identify the responsibilities and the parties involved to address complaints in the implementation of the program.
- Standards: There are a wide variety of standards emerging for IoT devices. Attestation approach is favorable because it permits the IoT developer to declare which standard is most appropriate to their product. However, since this is such a broad topic, it becomes important to validate that the standard selected is a) appropriate to the product and b) implemented correctly.

Other programs. Add a discussion on the possibility of incorporating the pilot labeling program in other programs. For example, the "Baseline Criteria for Consumer Software Cybersecurity Labeling program may be used by a certification body/inspection body to develop a new scheme or include in their existing cybersecurity scheme.

Regulatory/Purchasing Requirements. Add discussion on the possible application of the program by regulatory authorities and purchasing agreements. Encourage the adoption the program by both federal and state agencies in place of them developing their own requirements.

h) *Whether a template Declaration of Conformity would be useful for software providers.*

ANAB agrees that a template for the Declaration of Conformity will be helpful. A template will help with the consistency of the pilot program and answer questions that the software providers will have in preparing their SDoC.

A template will also provide a minimum standard for the content that must be included in the Declaration, in order for the declaration to be meaningful and comparable to other such declarations.

i) *Whether more details on evidence required to support assertions would be useful for software providers.*

Yes, details on acceptable levels of evidence and methods for capturing and documenting evidence should be provided.

In order for these labels to be meaningful, there must be rigor in the testing that occurs prior to the attestation of conformity to a label. A complaints-only enforcement process is too slow and onerous and will result in a loss of trust in the label.

As such, labels should either be awarded after consistent third-party testing has been passed or labels should be awarded after successful attestation where attestation requires a minimum level of evidence, including format, timestamps, and sampling for each requirement to which conformance is attested.

j) *Whether the technical baseline criteria are appropriate, including but not limited to:*

  - o *The feasibility, clarity, completeness, and appropriateness of attestations*
  - o *Normative references to be considered for inclusion*
  - o *Potentially requiring that the Software Identifiers attestation take the form of a Software ID Tags*

Technical baseline criteria are well selected and clear. In some instances, additional specificity of what is needed to meet the technical baseline criteria may benefit the consumer, for example:

- Vulnerability reporting / Free from Known Vulnerabilities: Labels relating to vulnerabilities should also include details as to which vulnerability scanning method was used, and which vulnerabilities were addressed (for example, all vulnerabilities or only critical ones). Additionally, there are multiple types of vulnerability scans:

  - Network vulnerability scanning
  - Application/code vulnerability scanning
  - Database and Server scans

Propose that the type of vulnerability scan be included in the label, or N/A if the type of scan is not applicable.

- Critical Cybersecurity Capability:
  - Consumers may benefit from being able to see the list of cybersecurity capabilities included in the product under its own section, so they can make informed choices about whether to invest in additional cybersecurity capabilities when using the product regardless of vulnerability status.
- Secure Development Process
  - Not all secure development processes are equivalent or appropriate to the product. Requiring developers to specify the secure development standard used to develop the product would add to the usefulness of this label.

3. Summary

ANAB supports the development of the “Draft Baseline Criteria for Consumer Software Cybersecurity Labeling” document. ANAB is prepared to work with NIST and other agencies in providing educational opportunities to aid in a better understanding of how conformity assessment works and can benefit the development of schemes to enhance the

Consumer Software Cybersecurity Labeling pilot program.