Enterprise Cloud Coalition ECC

December 16, 2021

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900
Email: labeling-eo@nist.gov

RE: ECC's Response to NIST's Draft Baseline Criteria for a Consumer Software Labeling Program

Dear NIST ITL Team:

The Enterprise Cloud Coalition (ECC) appreciates the opportunity to submit comments to the National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL) team on the Draft White Paper with Draft Baseline Criteria for Consumer Software Cybersecurity Labeling. [1]

ECC is comprised of enterprise-focused and cloud-based U.S. companies with shared business models based on processing data on behalf of other companies without monetizing user data for advertising. Taking advantage of the cloud-native features and functionality available through our solutions, ECC companies are directly involved in building and advancing technology that promotes innovation while providing ethical and consumer protection-related benefits to enterprises and their customers or users. As a result, ECC promotes those policies and standards that emphasize the privacy and security of data and information.

With the implementation of a Baseline Criteria for Consumer Software Cybersecurity Labeling program being mandated by Executive Order 14028, *Improving the Nation's Cybersecurity* (Cyber EO), for the specific purpose of changing the way in which consumers procure and use software and providers develop and secure their software, the reach and impact of this effort is wider than most of the other actions in the Cyber EO. With the potential to fundamentally change how the value of software is calculated, ECC commends NIST for seeking feedback from members of industry and the public.

To maximize the value of these labels to consumers, to incentivize the adoption of the framework by providers, and promote extensibility to Internet of Things (IoT) labeling where appropriate, NIST should: (1) Refine baseline criteria and attestations to maintain a clear, accessible, and objective standard; (2) Account for higher levels of audit rigor to incentive product improvement; and, perhaps most importantly, (3) Actively address the critical need for education among both consumers and providers to strengthen the credibility of the program.

Refine baseline criteria and attestations to maintain a clear, accessible, and objective standard

Besides making it easier for consumers to use and providers to adopt, doing so will also improve accessibility for non-English speakers and make it easier to adopt by small or startup businesses.

While the baseline criteria and associated attestations outlined in Section 2.3 are, for the most part, appropriate and effective for consumers, there are some questions that are raised by some of the individual attestations and a few

[1] National Institute of Standards and Technology (2021) DRAFT Baseline Criteria for Consumer Software Cybersecurity Labeling. (U.S. Department of Commerce, Washington, D.C.), NIST Draft White Paper, 1 November 2021. https://www.nist.gov/document/draft-baseline-criteria-consumer-software-cybersecurity-labeling

others that could be rewritten to come closer to an 8th grade reading level. The following are suggestions that should help achieve a clear, accessible, and objective standard that consumers and providers alike can understand.

2.3.1.1 Software Provider

The country where the provider is headquartered as well as where the individual within the entity responsible for the claims is located should be included. This would be useful for individuals who are at risk of being targeted by virtue of their position, whether they are an executive or an individual with clearance and access to sensitive information. Additionally, it would help to differentiate between products that are subject to differing rules and regulations by virtue of the provider's location, further incentivizing consumers to educate themselves on the utility of the information available through these labels. Consumer behaviors that change based on origin-related information would also provide an incentive for further harmonization among international standards, which itself would further incentive use of these labels by consumer and providers.

2.3.1.2 Label Scope

Templates that show how to describe the boundaries of software covered by attestations, focusing on examples of what is expected to be the most cited boundaries by providers in NIST's estimation, should be provided. Consumers would be able to have their own baseline by which to measure the label they are researching while providers would have a firm understanding of what would be expected in a complete, correct, and transparent assertion, further incentivizing both adoption and the ability to continuously improve upon the label itself. Consumer behaviors that change based on the scope of the attestation may also encourage providers to expand the scope of their reviews, incentivizing product improvement.

2.3.1.4 Attestation Date

While Section 3.1 lists a "date (year at a minimum)" as a component of a binary label, it should be made clear whether this attestation should represent the exact day on which the label was issued or not. Clarifying this will ensure consumers are aware of how "old" the attestation itself while also allowing providers the information necessary to understand how to adjust their own development process to accommodate for the frequency of which information will be shared with the public. Consumer behaviors that change – or don't – based on the date a label was issued should also provide useful datapoints for purposes of analyzing consumer awareness.

2.3.1.5 Software End of Support Date

Some software providers do not assign a fixed end of support date and others may have to account for circumstances that would require variable or different potential end of support dates. This is especially true in the open source community, where new versions and deprecations of old versions are not necessarily time boxed due to the nature of contributions to such a project. While the intended outcome is clear, the description and assertion as written will not support a significant portion of otherwise secure software components and products. Consumer behaviors that change based on a rewritten version of this assertion should be useful in providing a sense of what is a generally acceptable lifespan, further informing the necessary educational measures that will have to be undertaken with this program.

2.3.3.1 Free from Known Vulnerabilities

To provide some degree of measurability, this assertion should at least be tied to known vulnerabilities contained in the National Vulnerability Database (NVD). This would provide consumers and providers alike with an incentive to familiarize themselves with the NVD and the purpose it serves. It would also provide a baseline of known vulnerabilities that are accessible to anyone, without cost, and with vetted mitigation measures. Consumer behavior that is influenced by a provider's use of or contribution to the NVD will also make the NVD program itself more effective, which would in turn benefit the providers who rely on it as part of this attestation.

2.3.3.2 Software Integrity and Provenance

As quantum computing advances increase the potential that some of the current methods of encryption may be compromised, much like the Data Encryption Standard (DES) was, NIST should consider providing a reference to the appropriate modern cryptographic standard(s) that can be relied upon much like that which was made in 2.3.3.5. This

would allow for a consumer to be confident the signature itself was not tampered[2] with by malicious actors while also ensuring that providers can ensure they do not choose a less than optimal standard when developing an attestation-compliant update process. Consumer behavior that is seen to have been influenced by the knowledge that cryptographic standards must improve with time and that certain information should only be trusted to software that continues to meet the highest of security standards over time will be useful to develop and improve consumer awareness focused outreach or education efforts.

2.3.3.5 Strong Cryptography

The assertion should be modified to add the bold phrase, indicating that "software natively utilizes **or exceeds current** NIST approved cryptographic standards." As was discussed in 2.3.3.2, there will be a necessity to improve existing cryptographic standards in the relatively near future as quantum computing capabilities rapidly advance. With some consumer software, such as those in automobiles or appliances, intended to last for many years, there will be a real possibility that in a few years from now, a consumer must account for when software is using a deprecated versus a current cryptographic standard. Similarly, there will be instances where organizations working on the cutting edge of cryptography are able to attest, in good faith, that they are able to exceed the requirements associated with current NIST approved standards. Providing an opportunity to both understand absolute limitations while also accounting for improved methods of cryptography will incentivize product improvement and consumer awareness of the importance of cryptography itself. Consumer behavior that is impacted by the way in which cryptography is utilized can serve as an important data point for determining what educational resources will provide immediate value to those who have not yet adopted the labels.

2.3.4.1 Personally Identifiable Information (PII) Data Manifest

The desired outcome should be updated to also inform customers on whether their PII is monetized or otherwise used to generate revenue for the provider that is storing, processing, or transmitting such data. While a provider of software that monetizes the PII it controls or processes may use the best methods to secure that data available, if they rely on selling or otherwise providing access to it to others increases the potential for such data to ultimately end up in the hands of malicious actors due to a failure on the recipients' part. Consumers should be aware that there are security implications associated with using software that is incentivized to share their user's PII versus software that expressly disallows such use of this sensitive data. As we work to address "technical debt" associated with legacy systems and cybersecurity techniques, we must ensure that in our rush to build and store data in volumes never before seen, that we do not build up "privacy debt" that arguably poses a larger risk. Consumer behavior that is changed by relying on the privacy-related component of this attestation will improve consumer awareness of the implications of a breach and the importance of both security and privacy controls over their data.

2.3.4.2 Location Data Manifest

The same arguments and changes outlined in 2.3.4.1, above, apply to location data. Consumer awareness of the ease with which artificial intelligence and machine learning can be used to determine, with frightening accuracy, the precise identity of an individual by their location data is severely lacking and must be addressed. By building out additional privacy-focused goals as part of the desired outcome and required assertions, the rapidly accumulating "privacy debt" can be addressed in a significant manner. Consumer behavior that changes based on the increased awareness of the privacy and security implications will be an essential driver to incentive product improvement among providers.

2.3.4.3 Application-Specific Data Manifest

While the intention of this attestation to serve as a catch-all is relatively clear, adding language that the desired outcome would be to allow consumers to understand whether the safeguards used are focused on solely the security of data or both the security and privacy of that data.

[2] Note that in the Assertions of 2.3.3.2, there is a typo at the very end of the sentence: `tempered` is used instead of `tampered` for the second-to-last word.

Account for higher levels of rigor to incentivize product improvement

There is a very real difference between a self-assessment and an independent assessment that should be made clear to both consumers and providers.

Building on the USDA Organic label cited among the examples of binary label types on page 16, it should be noted that all meat, poultry, and eggs have a basic or "standard" label requirement[3] as is required by 9 CFR 317[4] and 381[5] that represents a bare minimum (i.e., baseline criteria) with the Organic label representing something above and beyond that bare minimum that keeps me from eating rotten food – or using insecure software. By using such a bifurcated process, NIST could maintain the binary label (i.e., a label that says you do meet the criteria established for expected consumption of food or software) while also providing an additional incentive or benefit that, while not exactly a tier, would provide an additional way to quickly gauge whether a particular software application was subject to a standard, self-assessment, or an independently verifiable, more rigorous one.

For those providers who choose to participate in this program and wish to either invest more heavily in their assessment process (e.g., establishing an internally-housed ISO-compliant conformity assessment team or using a third-party one) or portray the level of security they believe their industry should meet, higher levels of audit rigor should be rewarded with what would be the equivalent of an Organic label. Furthermore, differentiating between an "Organic" versus a "standard" label would help mitigate the "halo" effect to the extent that a product with either label will have met the same exact baseline process, while also providing a direct example of the different ways in which software can be secured for the "robust consumer education campaign" that is recognized as a key component for this effort's success.

Additionally, whether as part of the differentiation between "Organic" and "standard" or as part of a new Software Development Attestation, there should be an indication as to whether continuous monitoring or periodic monitoring is used, and if it is periodically, at what intervals that monitoring occurs. The rapid pace at which cyber criminals are developing new techniques and adopting emerging technologies to improve their success requires constant vigilance and awareness among consumers and providers alike and promoting the use of continuous monitoring in a way to at least meet control CA-7 outlined in NIST SP 800-161[6] will incentivize product improvement and increase consumer awareness of the associated security principles.

Actively address the critical need for education among both consumers and providers to strengthen the credibility of the program

Without a deeper understanding of the objectives this effort is intended to achieve and the way the labels reflect work towards those goals, the value of the labels will be diminished.

Beyond the various opportunities and specific lessons or topics that could be addressed from the suggestions provided throughout this response, there is a need for as much use case-based guidance as possible. Much like what the NIST Cybersecurity Centers of Excellence (NCCoE) and relatively similar efforts throughout the government have shown (e.g., DHS-PIL, Digital.gov, etc.) there is a real need for accessible and replicable resources that will help speed up the process to adopt most identified best practices in any field. These resources must not only be digestible, but they must also be accessible to practitioners at all levels of expertise.

---

[3] Food Safety and Inspection Service (2007) A Guide to Federal Food Labeling Requirements for Meat, Poultry, and Egg Products. (U.S. Department of Agriculture, Washington, D.C.), FSIS-GD-2007-0001, 1 August 2007. https://www.fsis.usda.gov/guidelines/2007-0001

[4] Labeling, Marking Devices, and Containers, 9 CFR 317 (1970, unless otherwise noted). https://www.ecfr.gov/current/title-9/chapter-III/subchapter-A/part-317

[5] Poultry Products Inspection Regulations, 9 CFR 381 (1972, unless otherwise noted). https://www.ecfr.gov/current/title-9/chapter-III/subchapter-A/part-381

[6] National Institute of Standards and Technology (2021) Supply Chain Risk Management Practices for Federal Information Systems and Organizations (U.S. Department of Commerce, Washington, D.C.), NIST SP 800-161 Rev. 1 (2nd Draft), 28 October 2021. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-draft2.pdf

With that in mind, a template Declaration of Conformity would be helpful, especially as it would provide a standard, baseline format, from which consumers and providers can educate themselves. Similarly, a template presenting the information consumers should have access to, including information listed in the Consumer Education-related bullets on page 18, and the type of content that would be deemed acceptable by regulators would be important for both types of stakeholders. This will not only provide the necessary guidance to comply with the baseline criteria, but also provide a format from which those who wish to learn more about the reasoning behind the criteria themselves can create a foundation for understanding based on the concepts NIST and industry participants in the feedback process have deemed necessary.

Finally, education for manufacturers and retailers are equally as important as consumers, and should, to the extent practicable within the context considered per the statement on page 19, borrow from as much of the consumer education program as possible. While it is understood each type of audience member will have specific informational needs, the core should be as similar as possible to ensure everyone that is a part of the labeling process is speaking in as similar terms as possible.

***

Again, ECC thanks NIST for the opportunity to provide feedback on the Draft Consumer Software Labeling Criteria and contributing to NIST's important work in improving the cybersecurity maturity of consumers and the developers of the software they use. We welcome questions on our feedback and look forward to continuing to be a part of this discussion as it develops.

Most sincerely,

Omid Ghaffari-Tabrizi
Enterprise Cloud Coalition
oghaffari@enterprisecloudcoalition.org
https://www.EnterpriseCloudCoalition.org/