kaspersky

# Comments Regarding Draft Baseline Criteria for Consumer Software

## Kaspersky's Submission

December 2021

---

### Introduction

We applaud the efforts of the National Institute of Standards and Technology (NIST), tasked by Executive Order (EO) 14028, in coordination with other agencies, to initiate pilot programs of cybersecurity labeling for consumer software. We are grateful for the opportunity to share our feedback to the Draft Baseline Criteria for Consumer Software Cybersecurity Labeling (further – the Draft), and hope our comments will be helpful in designing further guidance for software manufacturers and suppliers. Below, we share our comments to questions indicated by NIST as well as additional general comments. This submission complements our previously submitted comments[1] to the Draft Baseline Criteria for Consumer IoT Devices.

### Will the criteria achieve the goals of the EO by increasing consumer awareness and information, and will they help improve the cybersecurity of software which consumers purchase and use? Are the labeling-specific criteria appropriate and likely to be effective for consumers?

Unlike consumer IoT devices, modern software products are increasingly dynamic in nature, relying on multiple components – including those of third parties and open source libraries. Such a complex architecture of consumer software products represents an increased attack surface and, therefore, greater vulnerability; accordingly, software manufacturers should continuously implement cyber-risk monitoring and cyber third-party risk monitoring.

In this regard, labeling of consumer software products would unlikely be able to keep up with the pace of software's lifecycle, i.e., necessary changes, security configurations, and patch deployment, which can be performed practically every day.

Furthermore, for a label to serve as a useful tool to support consumers in making security-informed decisions, it should ideally rely on product ratings. These can help consumers compare software products on several criteria (for example functionality, performance, and cybersecurity), as people usually make their purchasing choices based on reviews rather than solely replying on just labels. For instance, in the cybersecurity industry, independent testing organizations such as AV-TEST[2] or AV-Comparatives [3] continuously conduct security evaluations and provide openly the results to help consumers make informed choices before purchasing cybersecurity solutions. Such organizations also apply the one and same methodology in security evaluations, so all products are compared using a single approach.

---

[1] Kaspersky's Comments to NIST Draft Baseline Criteria for Consumer IoT, October 2021
https://box.kaspersky.com/f/927e30c9489a40b8a508/?dl=1

2 www.av-test.org/en/?r=1

[3] www.av-comparatives.org

Therefore, we believe that labels complemented by such product ratings and reviews (based on security evaluations by third party independent organizations) can have a true positive security effect on consumers' behavior.

**Are the technical baseline criteria appropriate?**

Labels usually contain information with varying nature and updating speed. Practically speaking, the criterion 'Free from known vulnerabilities' should be updated regularly, while the criterion 'Implement a secure development process' can be updated rarely and does not require the same frequency of security attestations for a label.

Therefore, for a label to be feasible and realistic, and to serve the intended security purposes, we would recommend including information of the same nature and that which has to be updated with the same speed.

In addition to this, we believe that the criterion 'Free from known vulnerabilities' would unlikely be helpful for consumers since the information might be obsolete the day after the label has been issued. New information about known significant vulnerabilities appears every day, and this means that every day there is a risk of vulnerabilities appearing that may be significant or may affect a particular software product. If the software manufacturer has strong security controls and processes in place (such as vulnerability management and policies for coordinated vulnerability disclosure), this would serve as a sufficient security assurance that the manufacturer is able to effectively and timely respond to and mitigate vulnerabilities in its product. In addition, the presence of software component transparency processes (such as a software bill of materials) would be an additional essential artifact confirming the presence of sufficient security controls in the software development process and software delivery.

Therefore, we would recommend replacing the criterion 'Free from known vulnerabilities' to the criterion 'Protected from known vulnerabilities' where the assertions would include (but not be limited to):

- the presence of vulnerability management processes and policies
- the presence of coordinated vulnerability disclosure processes and policies
- the ability of the software manufacturer to produce and continuously maintain a software bill of materials
- presence of supply chain risk management controls as evidence of the manufacturer's ability to deal with third-party risks

**Conclusion**

We would like again to applaud the important work that NIST conducts by preparing the baseline security criteria for consumer software, and we hope our comments could be helpful for finalizing the draft criteria. In the meantime, we would be glad to provide additional information regarding the above if this may be needed.