MEMORANDUM

TO: National Institute of Standards and Technology
FROM: SecurityScorecard
Date: August 17, 2021
Re: Call for Papers on the Challenges and Practical Approaches to Consumer Software Labeling

SecurityScorecard, Inc. (SSC) is the global leader in cybersecurity ratings. We are grateful for the opportunity to submit the following comments in support of the National Institute of Standards and Technology's (NIST) efforts to identify practical approaches and address challenges to the development of a consumer software labeling program. This paper focuses on the merits of different product labeling programs for educating the public on the security properties of consumer software.

The constantly changing threat landscape and security postures of software developers require any labeling program to include continuous evaluation and dynamic scoring. Yet gathering, analyzing, categorizing and continuously monitoring internal security data of every software developer selling products into the U.S. market is a logistical impossibility. Nevertheless, SSC believes that there are a number of ways to leverage existing technologies to overcome many of these obstacles and provide the needed transparency for consumers.

We highlight two approaches that NIST can take: 1) developer self-assessments; or 2) independent assessments with the opportunity for developers to provide feedback and supplemental information. Each of these solutions also has dozens of potential iterations.

The first model - a trust but verify approach - requires NIST to set certain minimum standards across a range of cybersecurity controls and risk factors. NIST could develop easy-to-understand labels, using, for example, A-F or color-coded (e.g., platinum, gold, silver, bronze) grading systems. Companies developing software for use by the general public could then be required to include their grade at all online points of sale and/or on their website, with required periodic reassessments.

This approach has the advantage of being technology-agnostic and standards-based. Once the standards and tiers are developed, the agency managing this program would need to conduct periodic audits of companies' self-certification claims. Security ratings could support the agency by providing an outside-in view with which to compare companies' own self-assessments, allowing the agency to quickly identify and audit companies where the outside-in grade and a company's self-assessment grade are mismatched indicating potential errors in a self-certified claim. For example, companies that claim to meet the standards for an A or platinum rating, but that have a C or bronze grade or below from an independent cyber rating would be prioritized for audits. The private sector is likely to favor this standards-based, self-assessment approach.

Given resource constraints on the administering agency, however, it is likely that companies will be able to manipulate their ratings for extended periods of time before the agency in charge is able to audit and verify the findings. This could cause doubt among the public about the efficacy of ratings, reducing their effectiveness and utility. Independent verification entities could be employed to support the auditing effort, but without vigorous oversight and/or automating changes to company grades or labels, it will be exceedingly difficult to ensure the accuracy of grades on company websites and at online points of sale. Furthermore, the agency managing this program would also need to develop a method to capture the entire universe of software developers in order to ensure participation.

A second alternative would leverage existing technology like security ratings to develop independent assessments of software development security environments. These ratings could serve as an automated information base to rate every company's security hygiene. SSC, for example, already has 11 million entities rated globally, and we will have every company rated in the next 18-24 months. By scanning the internet daily with a global network of over 40 sensors, our ratings are supported by the most dynamic, continuously updated information available.

The executive branch agency charged with implementation could host a searchable website for consumers to look up the cyber ratings of the software developers. Feedback mechanisms could be built-in allowing companies to integrate inside-out information and contest possible inaccuracies to improve their grade, providing the agency with the ability to prioritize requests for score review based on risk, the effort associated with the review, and other relevant factors.

There are limitations to this concept as well. Security ratings provide a critical piece of information in the cyber hygiene puzzle, but they are an outside-in view of a company's cyber hygiene, and do not necessarily reflect the security of a particular software development environment.

Nevertheless, SSC can provide granular data on any environment with an IP address and attribute that IP address algorithmically with 95 percent accuracy so additional levels of detail are feasible. It is worth noting, too, that the security posture of the company is equally, if not more, important than the security posture of a particular software development environment. With 63 percent of breaches caused by third-party vendors, narrowly considering the security only of the development environment risks missing threats from broader company vulnerabilities.

Given the limitations of other conceptual frameworks, the impossibility of achieving 100 percent participation and accuracy, and the need for continuous monitoring, we believe that an automated, outside-in approach will come the closest to achieving the program's goals. This pilot program, "seeks to build on existing approaches and capabilities to avoid duplication and to speed implementation." SSC has developed a dynamic ratings system that builds trust in supply chains and third-party vendors and can serve as the backbone to NIST's labeling effort. We stand ready to iterate, provide data, and support this critical pilot program in any way.