SecurityScorecard

May 26, 2021

RE: Limited Comments of SecurityScorecard Responding to NIST's Call for Position Papers on Standards and Guidelines to Enhance Software Supply Chain Security

SecurityScorecard, Inc., the global leader in cybersecurity ratings with more than 5 million entities continuously rated, respectfully submits the following comments for the National Institute of Standards and Technology (NIST) efforts on the President's Executive Order on Improving the Cybersecurity of the Federal Government (14028), issued on May 12, 2021 (the "EO")[1]:

> *2. Initial list of secure software development lifecycle standards, best practices, and other guidelines acceptable for the development of software for purchase by the federal government.* This list of standards shall include criteria and required information for attestation of conformity by developers and suppliers. *See* EO Section 4(e)(i, ii, ix, and x).

American companies are dependent on software and computer networks for so many routine transactions, from managing billing to meeting basic communications with clients and customers. Each of these transactions has multiple dependencies and there is little transparency into the risks introduced by involved third, fourth, and fifth parties. Strengthening software security is a critical step towards improving the cybersecurity of public and private sector networks. Cybersecurity ratings are the only existing tool that can provide any degree of clarity on the cyber hygiene of every link in a supply chain, and must be identified as a software procurement best practice.

The EO states that "[t]he development of commercial software often lacks transparency, sufficient focus on the ability of the software to resist attack, and adequate controls to prevent tampering by malicious actors." Section 4(a). Indeed, unless every supplier is willing to open all of its networks for public inspection by any user and the federal government, buyers and downstream users have no ability to ensure that their suppliers are applying any best practices that NIST develops. As such, any development of best practices must first start with improved transparency.

We also applaud the White House for recognizing in Section 4(e)(1) of the EO the importance of the security of the software development environment: software is only as secure as the environment in which it is developed. Fair and transparent security ratings are currently the only tool available to government agencies and the private sector for objective, measurable, and publicly-available data about relevant development environments, and have been publicly endorsed as a valuable metric of cyber risk by various stakeholders, including in January 2021 by the Cybersecurity and Infrastructure Security Agency (CISA) National Risk Management Center.[2] In particular, CISA wrote:

> "The emergence of security ratings has driven cyber risk quantification as a way to calculate and measure cyber risk exposure. These security ratings provide a starting point for companies' cybersecurity capabilities and help elevate cyber risk to board decision making. Entities can also use security ratings alongside strategic risk metrics to align cyber scenarios with material business exposure; rollup cyber risks with financial exposure to inform risk management decisions; and

[1] The White House, *Executive Order on Improving the Nation's Cybersecurity*, May 12, 2021, available online at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[2] B. Kolasky, *A Risk-Based Approach to National Cybersecurity*, CISA blog (January 14, 2021), available online at: https://www.cisa.gov/blog/2021/01/14/risk-based-approach-national-cybersecurity.

SecurityScorecard, Inc.
Sachin S. Bansal, General Counsel
111 West 33rd Street. Floor 11
New York, NY 10001
sachin@securityscorecard.com
(646) 854-1188

measure improvement of cyber risk reduction over time. This kind of work needs to happen in the boardroom and also amongst national security leaders."[3]

CISA's recognition demonstrates how ratings must become an industry-standard best practice, which is already widely used in the private sector and gaining steam among state and federal agencies.

SecurityScorecard's A-F security ratings platform, like other leading security ratings platforms, are designed to bring transparency to organizations' cyber hygiene. Ratings are generated using publicly available data, weighted and combined with historical data, which produce an objective security score. SecurityScorecard has approximately 20,000 entity users worldwide; these organizations leverage security ratings to identify weaknesses in their own cyber hygiene and their vendor risk management programs. While a high score does not translate to immunity from cyber risk, poor scores are in fact strongly correlated with increased likelihood of breach or ransomware attack. This is unsurprising, as a poor score reflects that an organization has not sufficiently hardened its infrastructure against malicious actors.

Developing best practices in software assurance requires considering the security scores of software development environments. If a development environment is at risk, the security of the resulting software is put into question notwithstanding use of secure development methods. Criteria for evaluating secure software development environments must include their respective security ratings, especially in administratively separate build environments. While security ratings may not convey an exhaustive picture of an organization's cybersecurity posture, as certain controls remain behind firewalls, they can provide, at scale, a continuous, objective security measure of all organizations and demonstrate whether their security postures are improving or deteriorating over time.

In terms of security best practices, the Federal government should make use of security rating services to continually monitor the hygiene of its vendors. In addition to making use of security ratings, the government, or any end user of the software, should set a baseline for what the developer, or any third party, should assess and minimum requirements that should be met. Finally, the user should provide timely notice of deficiencies and require vendors to mitigate any perceived risks. Software developers should provide customers with a security rating for its development environment, and any evaluation of development procedures must consider the security rating of the development environment. Developers should also provide a mitigation plan or a detailed explanation of how internal compensating controls mitigate perceived risk(s).

As the global leader in security ratings, SecurityScorecard believes that ratings can bring the transparency called for in the EO to both the security posture of organizations and their software development environments. This will allow software developers to differentiate their products on not only price and capabilities, but also on the degree of security employed in their development phase, to, ultimately, improve the nation's cybersecurity. We welcome the opportunity to further address this issue during NIST's June 2-3 workshops.

Respectfully submitted,

Sachin S. Bansal

[3] *Id.*