SAFECode Response to NIST RFI about Evaluating and Improving Cybersecurity Resources

Steve Lipner
Executive Director, SAFECode
22 April 2022

SAFECode appreciates the opportunity to respond to the NIST Request for Information About Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework (CSF) and Cybersecurity Supply Chain Risk Management (SCRM). SAFECode is a non-profit organization focused on software security, secure development practices and on the security and integrity of software supply chains.

SAFECode has provided several comments on the NIST deliverables prepared in response to Executive Order 14028 on Improving the Nation's Cybersecurity and we were actively involved in the development and review of the NIST Secure Software Development Framework (SSDF). Our comments in response to the RFI focus on the software security and software supply chain aspects of the Cybersecurity Framework and NIST's guidance on SCRM.

The CSF has proven to be one of the most valuable and widely-used products of the NIST cybersecurity program. It has gained adoption worldwide and is widely viewed as providing actionable guidance for both governments and the private sector. Historically, the CSF has been silent about the importance and details of software security and secure development: the framework seems to assume secure software without commenting on how it is achieved or verified. It is indicative that the word "software" only appears four times in CSF Version 1.1.

The CSF does provide general high-level guidance on SCRM that is useful for software buyers but far from actionable by organizations concerned with software security and software supply chain. The CSF discussion of SCRM is silent about open-source software, and this omission is problematic given the role and importance of open-source in today's technology supply chain.

With regard to the software aspects of cybersecurity, the SSDF does an excellent job of providing guidance on both secure development and software supply chain. SAFECode believes that NIST should add one or more explicit call-outs to the SSDF in the introductory text and Framework Core of the CSF (not just in the Informative References). It is particularly important to include such call-outs in the CSF discussion of SCRM.

It would be useful to organizations seeking to use NIST guidance to implement software security programs if the discussion of Framework Implementation Tiers (Section 2.2) provided guidance that extended to the implementation of software security programs. This sort of guidance is also absent from the SSDF, and it would be especially valuable to smaller businesses (and again to open-source projects). There is no "finished" example of a family of implementation tiers for software security and supply chain, but we can point to the SAFECode document "Software Security and the CIS Controls" which defines "Development Groups" that are effectively implementation tiers, the Microsoft SDL Optimization Model, and the Google SLSA framework as useful resources to build on.

Our discussion above has focused on the CSF rather than NIST’s SCRM guidance. Overall, we believe that the CSF (and the SSDF) are especially practical and consumable by organizations, and thus we believe that NIST should build on those documents as it updates its guidance going forward. We also believe it is important for NIST to reflect international standards, which are widely accepted and implemented by private sector organizations worldwide.

Please feel free to contact us if you have any questions about this response.