April 29, 2022

Katherine MacFarland
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Via email to: CSF-SCRM-RFI@nist.gov

Subject: Open Source Security Foundation (OpenSSF)'s Comments on National Institute of Standards and Technology's Request for Information on Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

References: Docket Number: 220210-0045

Dear Ms. MacFarland:

The Open Source Security Foundation (OpenSSF) appreciates the opportunity to provide feedback on the National Institute for Science and Technology (NIST) Request for Information on *Evaluating and Improving NIST Cybersecurity Resources: Cybersecurity Framework and Cybersecurity Supply Chain Risk Management* (the RFI). We commend NIST's investment to update the Cybersecurity Framework (CSF) and to define the National Initiative for Improving Cybersecurity in Supply Chains (NIICS).

Hosted by the Linux Foundation, the OpenSSF (launched in August 2020) is a cross-industry organization that brings together the industry's most important open source security initiatives and the individuals and companies that support them. It combines the Linux Foundation's Core Infrastructure Initiative (CII), founded in response to the 2014 Heartbleed bug, and the Open Source Security Coalition, founded by the GitHub Security Lab to build a community to support open source security for decades to come. The OpenSSF is committed to collaboration and working both upstream and with existing communities to advance open source security for all. For more information, please visit: https://openssf.org/.

Founded in 2000, the Linux Foundation and its projects are supported by more than 1,800 members and is the world's leading home for collaboration on open source software, open standards, open data, and open hardware. Linux Foundation's projects are critical to the world's infrastructure, including Linux, Kubernetes, Node.js, Hyperledger, RISC-V, and more. The Linux Foundation's methodology focuses on leveraging best practices and addressing the needs of contributors, users, and solution providers to create sustainable models for open collaboration. For more information, please visit us at https://linuxfoundation.org.

The OpenSSF strongly supports the NIST CSF as a foundation for building trust and resiliency in software, regardless of its development model. It has proved itself as an effective tool (indeed, has become a global norm) for raising the general level of cyber awareness and building sound practices precisely because it provides a risk-based, flexible approach, allowing organizations to tailor and implement a cyber risk management program that is appropriate for their operational environments and level of risk and threats. It has been successful precisely because of the flexibility that comes with it.

Our comments below focus on addressing the National Initiative for Improving Cybersecurity in Supply Chains (NIICS) section of the RFI. When shaping NIICS, NIST should consider three themes relating to open source software: criticality of software lifecycle management, scaling supply chain risk management, and open source diversity.

Criticality of software lifecycle management

Software is pervasive across all aspects of life, and beyond the software that we interact with directly, software is also embedded within the hardware and services we use. Most software (regardless of its development model) is composed of other software, which a supplier may produce itself or acquire from a third-party, and each of those software components may be proprietary or open source. Those software components are also designed, developed, built, and published using other software and services.

Software might then be combined, re-packaged, bundled or incorporated into hardware, and then incorporated into systems and services acquired by the end user. This componentization and reuse accelerates innovation, promotes agility, and reduces costs but the resulting supply chain complexity can make defending it harder, especially using traditional supply chain risk management approaches.

It is critical to promote continuous software lifecycle management throughout the supply chain. The basic processes of understanding the software you have, where it is used, and the vulnerabilities it has are still performed inconsistently. These basic processes apply regardless of whether it is internal or product software development or the deployment of software. Failing to perform these basic processes consistently leads to vulnerabilities that can not only affect the user but can also be used to pivot to more critical assets or downstream users.

To account for the criticality of managing software lifecycles, including for open source software, the OpenSSF makes the following recommendations for NIICS:

- Provide practical guidance on how organizations, including government agencies, should use software component inventories as the foundation for software lifecycle management. This guidance should cover how to increase the accuracy, depth, and availability of dependency tracking information and how software bills of materials (SBOMs) might complement this information. It is important that this guidance be centered around the processes these artifacts support rather than the artifacts themselves.
- Supply chain risk management guidance and resources should guide users of all software to adopt appropriate compensating controls when direct or indirect suppliers are unable or unwilling to implement controls required by the consumers.

- Identify ways to amplify efforts from open source communities and industry, such as OpenSSF's Alpha/Omega project, to improve the security of open source projects and supply chains. This should include agencies evaluating their own use of open source and identifying how they can contribute to the security of this public good.
- Leverage existing Cybersecurity Framework (CSF) controls and mechanisms, such as the ID.SC category, to provide supplemental guidance on supply chain risk management (SCRM) for organizations already using CSF.

Scaling supply chain risk management

Supply chains use established norms, contractual requirements, legal obligations, voluntary certifications and standards, and market forces to elicit the desired behaviors between suppliers and consumers. Traditional supply chain risk management also encourages contract-based approaches as a means of mitigating third-party risk.

The pace, scale, diversity, and resulting complexity of supply chains for ICT products and services invites finding new or optimized approaches to supply chain risk management. Traditional approaches take a consumer-centric perspective and focus on defining requirements, establishing contracts with suppliers, and monitoring supplier performance. These approaches are necessary to create formal obligations but new approaches are also needed to provide faster detection of supply chain anomalies and to support new types of supply chain relationships, such as those with open source projects.

We believe that these new approaches are rooted in the transparent exchange of verifiable supply chain information as appropriate. Suppliers can generate artifacts describing the items they contribute to the supply chain as well as relevant information about their conformance to different requirements. Consumers can use this information, in conjunction with other risk management processes, to verify the item's integrity and make automated decisions about how an item can be used or to identify gaps with the consumer's requirements that they can either work with the supplier to remediate or compensate for.

Based on these considerations the OpenSSF makes the following recommendations for NIICS:

- Work with the entire open source ecosystem to identify low and no cost approaches and implementations, ideally automatable ones, that can be used in place of resource-intensive or costly conformance activities. Such tools should be open source, thereby increasing the breadth of adoption especially for resource-constrained organizations (such as open source projects and small businesses).
- Emphasize the use of automated assessment tools, such as OpenSSF's Scorecard[1] and Criticality Score[2] projects, to continuously assess open source dependencies. Automated assessment tools shouldn't be used to govern whether a project should or shouldn't be used but instead to identify areas of risk that warrant deeper investigation and to measure improvement over time.
- Identify additional guidance and standards needed to support agencies' consumption of SBOMs at scale, keeping in mind they are merely one element of software lifecycle management.

[1] https://openssf.org/blog/2020/11/06/security-scorecards-for-open-source-projects/
[2] https://openssf.org/blog/2021/05/03/introducing-the-security-metrics-project/

- Engage SBOM standards communities to provide guidance for software developers and agencies on how to produce and consume SBOMs.
- Identify investments in the National Vulnerability Database (NVD) that can leverage the information from SBOMs and improve integration with them.
- Investigate other supply chain information that may be exchanged through the supply chain in automated low-cost ways to support specific supply chain risk management processes. As part of this investigation existing solutions should be considered, for example, Sigstore[3] for signatures on software artifacts and SLSA[4] for attestations about supply chain artifacts.
- Provide guidance on how to produce supply chain information and how to consume it to support supply chain risk management processes.

Furthermore, Software Bills of Materials (SBOMs), as defined by *Executive Order 14028 (Improving the Nation's Cybersecurity)*, are a positive step in this direction. The Linux Foundation has supported SBOMs as demonstrated by its investment in the Software Package Data eXchange (SPDX) project which was published as an international open standard (ISO/IEC 5962:2021[5]) in 2021. The OpenSSF has also partnered with OWASP whose CycloneDX project is another popular SBOM specification.

We are at the beginning, not the end, of the SBOM journey. Discovering, transporting, and utilizing SBOMs at scale is still an emerging area and continuing to invest in these areas will be critical to SBOMs long-term success.

As we're investing in SBOMs it's important that we don't lose sight of their place in the overall supply chain process. SBOMs are an artifact produced by a supplier's asset management practices during the secure software development process and then used by the consumer's supply chain risk management processes. The investments in SBOMs, and any other supply chain information, should be in furtherance of specific supply chain risk management processes.

Open source diversity

Open source software is a global endeavor and requires diversity to succeed[6]. It is this non-discrimination that enables passionate individuals, research communities, governments, and organizations that compete with each other to collaborate, in the open, to move technology (and hopefully society) forwards. An open source project, which may be governed by formal or informal groups of people or organizations, will have contributors from varying backgrounds and locations. The contributors to these projects change organically over time and many small projects have only a single contributor while large projects often receive many single contributions from contributors.

Each software ecosystem is unique and shaped by its community and technical values, vision, and resources. Sometimes these are explicitly decided and sometimes they evolve organically over the ecosystem's life. For

[3] https://www.sigstore.dev/
[4] https://slsa.dev/
[5] https://www.iso.org/standard/81870.html
[6] https://opensource.org/osd

example, one software ecosystem might value smaller updates more frequently and another might value larger updates less frequently. There is rarely one singular correct way to approach a problem and instead potential solutions are weighted based on the community's values, available resources, and risk tolerance.

The diversity of open source projects is also reflected in the diversity of their business and funding models, and the level of funding open source projects receive does not necessarily correlate to their criticality and breadth of use. When considering approaches to supply chain risk management that require suppliers to commit resources, financial or otherwise, special consideration needs to be given to how these approaches apply or affect open source projects with limited resources.

Based on these considerations the OpenSSF makes the following recommendations for NIICS:

- Solicit input from a diverse selection of open source ecosystem participants including users, vendors, service providers, and open source projects and foundations for their perspectives on supply chain security issues.
- Supply chain risk management resources should consider both the proprietary software and open source software models and provide practical control implementation guidance for suppliers with constrained resources..
- Supply chain risk management guidance and resources should consider both direct and indirect dependencies and how differing security postures and the increased difficulty in affecting change on indirect dependencies impacts approaches to supply chain risk management.
- Engage international standards and government bodies that are, or are considering, developing standards related to supply chain security and promote coherent and holistic approaches.

The OpenSSF encourages NIST to continue conducting multi-stakeholder engagements to define the National Initiative for Improving Cybersecurity in Supply Chains (NIICS). We and OpenSSF members welcome the opportunity to participate in those engagements and look forward to collaborating and providing our open source security perspectives.

Respectfully,

Brian Behlendorf
GM, OpenSSF, speaking on behalf of the Governing Board and Public Policy Committee
Open Source Security Foundation (OpenSSF)
a Linux Foundation Project