Carnegie Mellon University
Software Engineering Institute

RESPONSE TO OFFICE OF NATIONAL CYBER DIRECTOR REQUEST FOR COMMENT ON OPEN-SOURCE SOFTWARE SECURITY AND MEMORY SAFE PROGRAMMING LANGUAGES

Brett Tucker, Scott Hissam, Hasan Yasar, Joseph Yankel, Robert Schiela
October 2023

Introduction

The Software Engineering Institute (SEI) at Carnegie Mellon University is a Federally Funded Research and Development Center (FFRDC) that is committed to the advancement of practice in software engineering and cybersecurity. Open-Source Software (OSS) provides significant opportunities for the global community of programmers, software developers, and customers by providing mostly useful, prepackaged algorithms and coded programs that enable rapid development of all varieties of applications. Unfortunately, those benefits may be offset by risk exposure for consumers who may be unaware of malicious and non-malicious elements found within the products used. This document captures the response of the SEI to the United States White House Open-Source Software Security Initiative (OS3I) request for information that was issued in August 2023. In summary, the SEI recognizes the greatest value and priority for the United States Government (USG) to focus upon Secure OSS Foundations along with OSS Communities and Governance followed by other areas provided. Finally, the SEI shares some additional contributions to novel policy and economic considerations.

First Priority – Secure the Supply Chain

Given the tremendous reliance of the USG upon third party providers, their tertiary suppliers, and all other supply chain stakeholders, the SEI recognizes the greatest value and appropriate focus should be given to reducing classes of vulnerabilities at scale. More specifically, the USG should seek to strengthen the software supply chain. By doing so, the USG can establish greater confidence in its existing code base as much as assessing and responding to new technologies, products, and vendors that provide great benefit. As a sub-area, the SEI would recommend strengthening the software supply

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

chain by seeking out and supporting novel tools and methodologies that detect and mitigate vulnerabilities found within OSS products. Furthermore, organizations must be able to track, scan, and manage vulnerabilities with a Zero Trust ethos in mind.

Given known minimum elements for Software Bills of Materials (SBOMs), more specific direction for application of that information would help the OSS consumer base with standardized best practices for management of a code base supported by OSS elements. The SEI suggests the application of a capability maturity model that matches practices and policies with the capability, scope, and scale of service providers. As a distant aspiration, the SEI envisions application of such a model to provide direction for improved resilience and possibly assessment frameworks that guide security attestations by OSS providers and consumers. From its experiences in developing previous maturity models and assessment methodologies, the SEI estimates that the USG could fuel the development of such models with modest sums in the millions to tens of millions of dollars range for any number of FFRDC, national laboratory, UARC, or private organization development and support. Analogous application of assessment and maturity rating for secure practices may be found in the development of the Department of Defense Cybersecurity Maturity Model Certification (CMMC) program.

The secure software supply chain area shares a lot of overlap with reducing entire classes of vulnerabilities at scale as a sub-area. Specifically, the USG may leverage maturity models to compel best practices, especially if those models are mandates for use by the USG supplier base. Secure by design, secure by default, validation practices, and other related considerations may require regulatory policy or market pressure to find ubiquitous use where incentivization fails.

Secondary Considerations

Once methodologies exist for measuring the scope and scale of the challenges for legacy technical debt and assessment of new technology, the USG may then seek more extensive changes that hinge upon human behavior and choice. For example, the RFI contains sub-areas that push for large scale adoption of memory safe languages. While noble and necessary, the SEI recognizes deprecated value compared to the first priority, since workforce development, skillset development, and education takes longer periods of time and more grassroots appeal for implementation. Before significant investment takes place, the SEI recommends that the USG consider the limits of memory safe languages by asking if such languages can guarantee reduction of all risk to acceptable levels let alone zero. Please note that the SEI does not doubt the value of Rust, Python, and other memory-safe languages at hand. Rather, the SEI recognizes the degree of difficulty experienced by schools, training programs, and other educators in shaping a responsible programming professional.

Safely assuming that memory safe programming languages demonstrate return on investment, the SEI can identify influential organizations such as the US Department of Education and the National Science Foundation that may serve as vehicles for distribution of resources to educators, trade schools, professional organizations, and the like that play active roles in forging a dedicated workforce. The

SEI estimates hundreds of millions of dollars spent consistently over years to fund workforce development efforts. A multi-pronged approach starts with influencing future workforce employees at the primary school and trade school level, teaching new coding languages as well as secure methods for programming. The same level of support should be applied in subsidy to collegiate institutions. The USG could also influence existing members of the workforce by endorsing professional organizations, licensing bodies, and certification providers to mandate memory safe language and programming practices (e.g., Development Security Operations). Similarly, large software foundries and product developers may be subsidized to deliver training programs for secure coding and engineering practices.

Latter Considerations

Although important, the SEI recognizes far more strategic plays that deserve attention but should be engaged with greater scrutiny and consideration for return on risk investment. For example, the SEI sees value in the utilization of Large Language Models (LLMs) to assist in converting existing code bases to memory safe languages. Conversion, however, presents many challenges for proper model training and follow-on testing to ensure proper functionality once converted. In these cases, automated conversion is only a first step in activity for a process that would require many skilled professionals otherwise burdened with projects that have greater promise for financial gain.

Similarly, the SEI values the notion of engaging international partners to build a stronger and more robust community that is dedicated to secure software products. For example, there is strategic benefit to allaying the use of OSS with origins in generally accepted threat actor countries such as Russia and China. However, given the independent agendas of foreign nations and having expectation that those governments possess the same level and degree of power to effect changes within their own independent OSS communities is speculative when compared to addressing the immediate needs of the USG and its own indigenous provider base. The SEI sees value in taking initial steps stated above and levering the lessons learned when projecting its diplomacy with partner nations. This does not discount the ability of the USG to multi-task, but a phased approach may be called upon to maximize the impacts driven by diplomacy and other collaborative intents. Furthermore, the USG would be wise to learn from the European Union and other regions as they seek to achieve the same degree of assurance and trust in its codebase.

Legal Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

DM23-0970

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412/268.5800 | 888.201.4479
Web: www.sei.cmu.edu
Email: info@sei.cmu.edu