EXECUTIVE OFFICE OF THE PRESIDENT

Office of the National Cyber Director

Request for Information on Open-Source Software Security: Areas of Long-Term Focus and Prioritization

AGENCY: Office of the National Cyber Director, Executive Office of the President, Cybersecurity and Infrastructure Security Agency, DHS, National Science Foundation, Defense Advanced Research Projects Agency, and Office of Management and Budget, Executive Office of the President.

ACTION: Request for information (RFI).

SUMMARY:

The Office of the National Cyber Director (ONCD), the Cybersecurity Infrastructure Security Agency (CISA), the National Science Foundation (NSF), the Defense Advanced Research Projects Agency (DARPA), and the Office of Management and Budget (OMB) invite public comments on areas of long-term focus and prioritization on open-source software security.

DATES: Comments must be received in writing by 5 pm ET October 9, 2023.

ADDRESSES: Interested parties may submit comments through www.regulations.gov. For detailed instructions on submitting comments and additional information on this process, see the SUPPLEMENTARY INFORMATION section of this document.

FOR FURTHER INFORMATION CONTACT: Requests for additional information may be sent to: OS3IRFI@ncd.eop.gov, Nasreen Djouini, telephone: 202-881-4697.

SUPPLEMENTARY INFORMATION:

As highlighted in the National Cybersecurity Strategy (https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf), and its Implementation Plan Initiative 4.2.1, the ONCD has established an Open-Source Software Security Initiative (OS3I) to champion the adoption of memory safe programming languages and open-source software security. The security and resiliency of open-source software is a national security, economic, and a technology innovation imperative. Because open-source software plays a vital and ubiquitous role across the federal government and critical infrastructure,[1] vulnerabilities in open-source software components may cause widespread downstream detrimental effects. The federal government recognizes the immense benefits of open-source software, which enables software development at an incredible pace and fosters significant innovation and collaboration. In light of these factors, as well as the status of open-source software as a free public good, it may be appropriate to make open-source software a national public priority to help ensure the security, sustainability, and health of the open-source software ecosystem.

[1] "2023 Open-Source Security and Risk Analysis Report," Synopsys, February 22, 2023, (https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html?utm_source=bing&utm_medium=cpc&utm_term=&utm_campaign=B_S_OSSRA_BMM&cmp=ps-SIG-B_S_OSSRA_BMM&msclkid=15e8216ad16511c8b01945c7b683c395)

In 2021, following the aftermath of the Log4Shell vulnerability, ONCD in collaboration with the Office of Management and Budget's (OMB) Office of the Federal Chief Information Officer (OFCIO), established the Open-Source Software Security Initiative (OS3I) interagency working group with the goal of channeling government resources to foster greater open-source software security. Since then, OS3I has welcomed many other interagency partners, including the Cybersecurity Infrastructure Security Agency (CISA), the National Science Foundation (NSF), Defense Advanced Research Projects Agency (DARPA), National Institute of Standards and Technology (NIST), Center for Medicare & Medicaid Services (CMS), and Lawrence Livermore National Laboratory (LLNL) in order to identify open-source software security priorities and implement policy solutions.

Over the past year, OS3I identified several focus areas, including: (1) reducing the proliferation of memory unsafe programming languages; (2) designing implementation requirements for secure and privacy-preserving security attestations; and (3) identifying new focus areas for prioritization.

This Request for Information (RFI) aims to further the work of OS3I by identifying areas most appropriate to focus government priorities, and addressing critical questions such as:

- How should the federal government contribute to driving down the most important systemic risks in open-source software?
- How can the federal government help foster the long-term sustainability of open-source software communities?
- How should open-source software security solutions be implemented from a technical and resourcing perspective?

This RFI represents a continuation of OS3I's efforts to gather input from a broad array of stakeholders.

Three-Phase RFI Approach

For this RFI, the Government intends to engage with interested parties in three phases:

Phase I – Addressing Respondent Questions About this RFI

- If you have any questions about the context of the Government's RFI, the processes described, or the numbered topics below, you may send them to OS3IRFI@ncd.eop.gov by August 18, 2023.
- By August 28, 2023, the Government will post responses to select questions on www.regulations.gov, as appropriate.

Phase II – Submittal of Responses to the RFI by Interested Respondents

- By October 9, 2023, all interested respondents should submit a written RFI response, in MS Word or PDF format, focusing on questions for which they have expertise and insights for the Government (no longer than 10 pages typed, size eleven font) to www.regulations.gov with the email subject header "Open-Source Software Security RFI Response" and your organization's name.
- Title page, cover letter, table of contents, and appendix are not included within the 10-page limit. In the body of the email, also include contact information for your organization (POC Name, Title, Phone, Email, Organization Name, and Organization Address).

Phase III – Government Review

- The Government reviews and publishes the RFI responses submitted during Phase II. The Government may select respondents to engage with the RFI project team to elaborate on their response to the RFI.

Participation, or lack thereof, in this RFI process has no bearing on a party's ability or option to choose to participate in or receive an award for any future solicitation or procurement resulting from this or any other activity.

Questions for Respondents:

We are seeking insights and recommendations as to how the federal government can lead, assist, or encourage other key stakeholders to advance progress in the potential areas of focus described below.

Please consider providing input on these areas by addressing the questions below:

- Which of the potential areas and sub-areas of focus described below should be prioritized for any potential action? Please describe specific policy solutions and estimated budget and timeline required for implementation.
- What areas of focus are the most time-sensitive or should be developed first?
- What technical, policy or economic challenges must the Government consider when implementing these solutions?
- Which of the potential areas and sub-areas of focus described below should be applied to other domains? How might your policy solutions differ?

Respondents are not required to respond to every topic and are encouraged to focus on specific areas that meet their specialized expertise.

Potential Areas of Focus

- Area: Secure Open-Source Software Foundations
    - Sub-area: Fostering the adoption of memory safe programming languages
        - Supporting rewrites of critical open-source software components in memory safe languages
        - Addressing software, hardware, and database interdependencies when refactoring open-source software to memory safe languages
        - Developing tools to automate and accelerate the refactoring of open-source software components to memory safe languages, including code verification techniques
        - Other solutions to support this sub-area
    - Sub-Area: Reducing entire classes of vulnerabilities at scale
        - Increasing secure by default configurations for open-source software development
        - Fostering open-source software development best practices, including but not limited to input validation practices
        - Identifying methods to incentivize scalable monitoring and verification efforts of open-source software by voluntary communities and/or public-private partnerships
        - Other solutions to support this sub-area

    - Sub-Area: Strengthening the software supply chain
        - Designing tools to enable secure, privacy-preserving security attestations from software vendors, including their suppliers and open-source software maintainers
        - Detection and mitigation of vulnerable and malicious software development operations and behaviors
        - Incorporating automated tracking and updates of complex code dependencies
        - Incorporating zero trust architecture into the open-source software ecosystem
        - Other solutions to support this sub-area
    - Sub-Area: Developer education
        - Integrating security and open-source software education into computer science and software development curricula
        - Training software developers on security best practices
        - Training software developers on memory safe programming languages
        - Other solutions to support this sub-area
- Area: Sustaining Open-Source Software Communities and Governance
    - Sustaining the open-source software ecosystem (including developer communities, non-profit investors, and academia) to ensure that critical open-source software components have robust maintenance plans and governance structures
    - Other solutions to support this sub-area

- Area: Behavioral and Economic Incentives to Secure the Open-Source Software Ecosystem
    - Frameworks and models for software developer compensation that incentivize secure software development practices
    - Applications of cybersecurity insurance and appropriately-tailored software liability as mechanisms to incentivize secure software development and operational environment practices
    - Other solutions to support this sub-area
- Area: R&D / Innovation
    - Application of artificial intelligence and machine learning techniques to enhance and accelerate cybersecurity best practices with respect to secure software development
    - Other solutions to support this sub-area
- Area: International Collaboration
    - Methods for identifying and harmonizing shared international priorities and dependencies
    - Structures for intergovernmental collaboration and collaboration with various open-source software communities
    - Other solutions to support this sub-area

This RFI seeks public input as the Federal government develops its strategy and action plan to strengthen the open-source software ecosystem. We hope that potential respondents will view this RFI as a civic opportunity to help shape the government's thinking about open-source software security.

Comments must be received no later than 5:00 pm ET October 9, 2023.

By October 9, 2023, all interested respondents should submit a written RFI response, in MS Word or PDF format, with their answers to questions on which they have expertise and insights for the Government through www.regulations.gov.

The written RFI response should address ONLY the topics for which the respondent has expertise. Inputs that meet most of the following criteria will be considered most valuable:

- Easy for executives to review and understand: Content that is modularly organized and presented in such a fashion that it can be readily lifted (by topic area) and shared with relevant executive stakeholders in an easily consumable format.
- Expert: The Government, through this effort, is seeking insights to understand current best practices and approaches applicable to the above topics, as well as new and emerging solutions. The written RFI response should address ONLY the topics for which the respondent has knowledge or expertise.
- Clearly worded/not vague: Clear, descriptive, and concise language is appreciated. Please avoid generalities and vague statements.
- Actionable: Please provide enough high-level detail so that we can understand how to apply the information you provide. Wherever possible, please provide credible data and specific examples to support your views. If you cite academic or other studies, they should be publicly available to be considered.
- Cost effective & impactful: Respondents should consider whether their suggestions have a clear return on investment that can be articulated to secure funding and support.

- "Gordian Knot" solutions and ideas: Occasionally, challenges that seem to be intractable and overwhelmingly complex can be resolved with a change in perspective that unlocks hidden opportunities and aligns stakeholder interests. We welcome these ideas as well.
- All submissions are public records and may be published on www.regulations.gov. Do NOT submit sensitive, confidential, or personally identifiable information.

An additional appendix of no more than 5 pages long may also be included. This section should only include additional context about you or your organization.

Privacy Act Statement:

Submission of comments is voluntary. The information will be used to determine focus and priority areas for open-source software security and memory-safety. Please note that all comments received in response to this notice will be posted in their entirety to https://www.regulations.gov, including any personal and business confidential information provided. Do not include any information you would not like to be made publicly available.

Kemba E. Walden

Acting National Cyber Director