November 9, 2023

Kemba E. Walden
Acting National Cyber Director
Office of the National Cyber Director (ONCD)
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, D.C. 20504

Re: FR Doc. 2023–17239, "Request for Information: Open-Source Software Security: Areas of Long-Term Focus and Prioritization"

Dear Acting National Cyber Director Walden:

Hedera Hashgraph, LLC (also known as the "Hedera Council") the multi-stakeholder governing body of the the open source, public distributed ledger built on the hashgraph algorithm (known as the "Hedera Network") is pleased to submit this response to the White House Office of the National Cyber Director (ONCD), Cybersecurity Infrastructure Security Agency (CISA), National Science Foundation (NSF), Defense Advanced Research Projects Agency (DARPA), and Office of Management and Budget's (OMB) Request for Information (RFI) on *"Open-Source Software Security and Memory Safe Programming Languages."* We appreciate the opportunity to engage in this dialogue with the Administration to share insights on open source development, memory safe programming languages, and vital risk mitigation measures. As an enterprise consortium governing an open source, leaderless, proof-of-stake public ledger platform (also known as a "blockchain"), enabling scalable enterprise applications for our members and their peers around the world, the security of our open source software is fundamental.

Open source is not only a set of licenses that grant certain rights but a set of behaviors based on meritocracy, collaboration and transparency — critical elements in building a trusted software ecosystem. Open source project leadership values individuals and organizations that engage in a manner aligned to well-established open source principles. Various government agencies have demonstrated a clear understanding of these principles by contributing key innovations back to the open source communities they participate in, hiring experienced open source contributors, and actively seeking feedback directly from the communities they participate in. We offer several suggestions for how the U.S. government can deepen this capability while simultaneously strengthening open source software security.

Create an Open Source Program Office to Lead Federal Open Source Activity

We suggest CISA consider creating the equivalent of an Open Source Program Office (OSPO), to coordinate activities across the 20+ various federal agencies engaged in improving their open source software cybersecurity. These expanded OSPO activities would include:

- Engage — Coordinate mid to senior level federal agency engagement across relevant projects and foundations. This has proven particularly useful in the commercial open source ecosystem when leaders get directly involved.
- Understand — Collect and analyze the various cyber risks the agencies have identified with open source software they rely upon, their specific software development processes, the relevant threat models and mitigation strategies, and contribute this enhanced analysis back to both the agencies and the open source communities themselves.
- Contribute — Identify existing process barriers holding back agency employees and contractors from fully participating in public open source communities and facilitate policy changes that would remove such barriers, making direct open source community involvement as easy as practicable for government employees and contractors.

Identify Strategic Intersections to Guide the Future of Open Source Security

We also suggest increasing U.S. government participation in industry consortia, communities and foundations to analyze the underlying pivotal intersections between open source processes and their impact on future technologies. We suggest supporting the following activities with industry groups:

- Research & Analysis: Conduct studies to identify the most vulnerable processes in popular open source software development ecosystems.
- Legacy Systems: Identify opportunities for key legacy systems to be enhanced by the open source development of common interfaces that benefit from modern approaches to cybersecurity.
- Funding Initiatives: Develop a transparent framework for prioritizing modernization opportunities in U.S. systems through open source development based on factors such as potential security impact, the number of users affected, and allocate funding through grants and bounties specifically targeted at the high-priority opportunities identified.
- Communication Channels: Actively engage in existing communication channels (open source community newsletters, webinars, community forums, etc.) to keep the broad community informed of U.S. agency priorities and the progress you are making against these publicly disclosed modernization objectives to maximize community engagement and support of those objectives.

Promote the Use of Memory Safe Programming Languages

Given that well over 60% of 0-day vulnerabilities in popular operating systems are due to memory safety language vulnerabilities and related risks that can result in unstable systems,[1] we appreciate the continued U.S. government emphasis on this topic to improve software cybersecurity.

Activities the U.S. government could take to promote the use of memory safe languages include:

- Grants and Scholarships: Offer grants for projects that focus on developing, improving, or promoting memory safe programming languages, or that are building tooling to make them easier to use for application development.
- Code Audits and Reviews: Offer free or subsidized code reviews for open source projects written in memory-safe languages.
- Curriculum Development: Partner with educational institutions to introduce or expand the teaching of memory-safe languages in computer science programs at all levels of science education.
- Developer Training Programs: Launch specialized courses for developers interested in development using memory-safe languages. Offer secure-by-design training for open source developers.

Collaborate with Industry to Establish Open Source Software Attestation Standards

Open source software attestations come in two forms, both providing trusted authentication of metadata about a software artifact: 1) attestation that there are no known vulnerabilities in the software; and 2) attestation as to the composition of a software build, commonly referred to as a SBOM (Software Bill of Materials). Both techniques can provide useful cybersecurity risk mitigation capabilities to systems relying upon open source software.

Coordinated through the CISA OSPO, the government could work with industry to craft standards, implementation schemes, training, and monitoring programs for the use of such attestations within the open source Software Development Life Cycle (SDLC). Activities could include:

- Standardize Requirements: Develop a universally accepted set of requirements for security attestations.
- Privacy Framework: Adopt a privacy-preserving framework, such as Zero-Knowledge Proofs (ZKPs), to ensure that security attestations don't compromise private data.
- Open Source Reference Implementations: Release reference code for privacy-preserving security attestations to encourage adoption by project developers.

---

[1] https://www.memorysafety.org/docs/memory-safety/#:~:text=An%20analysis%20of%200%2Ddays,were%20memory%20safety%20issues%201.

- Regular Audits: Establish a subsidized, recurring audit process for projects using the attestation framework to ensure compliance and maintain trust.
- Education: Provide training and resources for developers to understand and implement the privacy-preserving security attestation requirements.
- Feedback Loop: Establish channels for feedback from the developer community to continually refine and update the attestation requirements and tooling.
- Code Integrity: Ensure popular mechanisms that validate the completeness and integrity of open source code leverage these privacy-preserving security attestation standards.

Conclusion

We welcome the opportunity for further dialogue regarding open source security, and how the Hedera Network open source community can collaborate with the Administration to foster the long-term sustainability of open source platforms that enable enterprise applications for both the public and private sector.

Sincerely,

Andrew Aitken
Chief Open Source Officer
Hedera Hashgraph, LLC