SUMMARY OF THE 2023 REQUEST FOR INFORMATION ON OPEN-SOURCE SOFTWARE SECURITY

AUGUST 2024

THE WHITE HOUSE
WASHINGTON

CMS.gov

Science and Technology

U.S. DEPARTMENT OF ENERGY

OPEN–SOURCE SOFTWARE SECURITY RFI SUMMARY

ACKNOWLEDGEMENTS

This Summary of the 2023 Open-Source Software Security Request for Information Report (RFI) is an outcome of the vast amount of time, energy, and expertise dedicated by U.S. federal government representatives from the Open-Source Software Security Initiative (OS3I). We offer our sincerest gratitude to the technical and policy experts that undertook the analysis of the RFI submissions from the Center for Medicare and Medicaid Services (CMS), Cybersecurity and Infrastructure Security Agency (CISA), Defense Advanced Research Projects Agency (DARPA), Department of Homeland Security (DHS), General Services Administration (GSA), Lawrence Livermore National Laboratory (LLNL), National Institutes of Standards and Technology (NIST), National Science Foundation (NSF), National Security Agency (NSA), Office of the Director of National Intelligence (ODNI), Office of Management and Budget (OMB), Office of the National Cyber Director (ONCD), Office of Science & Technology Policy (OSTP), Office of Secretary of Defense, Chief Digital Artificial Intelligence Office - Defense Digital Service (DDS).

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In August of 2023, ONCD, CISA, NSF, DARPA, and OMB published a Request for Information (RFI) on Open-Source Software Security in the Federal Register.[i]

The RFI closed for public comment on November 8, 2023. Respondents provided one hundred and seven public submissions addressing five areas the Federal Government should prioritize to improve the security of the open-source software ecosystem. RFI submissions advocated for a considerable number of Federal Government actions, including:

1. Increase the adoption of memory-safe programming languages and, using a tiered and prioritized approach, translate open-source software libraries to memory-safe programming languages.
2. Fund the development of new open-source tools and libraries to help secure the open-source software ecosystem.
3. Research the use of Artificial Intelligence (AI), including Large Language Models (LLMs) and Machine Learning (ML), to enhance and accelerate secure software development.
4. Pursue public-private partnerships within open-source software development ecosystems.
5. Share known vulnerabilities throughout the global software supply chain.
6. Invest in educating new and existing developer talent to pursue secure open-source software projects and initiatives.
7. Foster international collaboration with other governments, agencies, and organizations on open-source software policies and frameworks that work across borders.
8. Leverage existing policies and frameworks to inform procurement requirements for open-source software projects and initiatives.

Since 2022, ONCD has convened the Open-Source Software Security Initiative (OS3I) Working Group to drive policy solutions to secure and defend the open-source software ecosystem. This summary report provides background on the impetus behind the RFI and then summarizes submissions by recommendations for each focus area. Next, the report identifies Federal Government activities that align with the RFI recommendations and lays out the work ahead in the year to come, detailing initiatives with other government agencies, the open-source software community, and the private sector to build toward a more secure and prosperous digital future.

BACKGROUND

American economic prosperity thrives on innovation that is enabled by the open-source software ecosystem. The President's National Cybersecurity Strategy emphasizes the need to work with the private sector and the open-source software community, and to sustain investment to achieve a more defensible and resilient digital ecosystem.[ii] A key feature of the open-source software community is that it is driven by collaboration, transparency, and trust — all necessary ingredients for innovation. At the same time, the widespread use and adoption of open-source software has drawn the attention of threat actors for exploitation across the software supply chain. The 2021 Log4Shell vulnerability and the 2024 XZ Utils backdoor demonstrate the potential for systemic impact when sustained security is not prioritized.[iii] It is imperative to bolster the security and resilience of the open-source software ecosystem while preserving the key features that foster innovation and economic prosperity.

Since 2022, ONCD has convened the OS3I Working Group to drive policy solutions to secure and defend the open-source software ecosystem. Through the OS3I, the Federal Government has amplified its efforts to push forward key implementation initiatives on open-source software security.[iv] These initiatives highlight the advantage of coordinated investment and collaboration with the open-source software community, industry, and civil society.

In 2023, ONCD, CISA, NSF, DARPA, and OMB issued an RFI to gather recommendations from the open-source software community on areas for long-term focus and prioritization to secure the open-source software ecosystem. The RFI received one hundred and seven public responses addressing five identified focus areas the Federal Government should prioritize to improve resiliency: (i) Secure Open-Source Software Foundations; (ii) Sustaining Open-Source Software Communities and Governance; (iii) Behavioral and Economic Incentives to Secure the Open-Source Software Ecosystem; (iv) R&D/Innovation; and (v) International Collaboration. Respondents to the RFI were not required to answer each question, and the majority of responses concentrated on focus area one: secure open-source software foundations. The summary report illustrates key findings of submissions according to each focus area (Chart 1.1). This is followed by an in-depth summary of the recommendations received. Next, the report outlines OS3I activities that align with the RFI recommendations.

The government has heard the community and is mobilizing on these recommendations. OS3I actions include twelve activities that members of the OS3I plan to complete—or have completed—in 2024. These activities include: (1) Advance research and development; (2) Secure package repositories; (3) Partner with open-source software communities; (4) Promote further development and implementation of the use of Software Bill of Materials (SBOMs); (5) Strengthen the software supply chain; (6) Establish the first U.S Government Open-Source Program Office (OSPO); (7) Assign vulnerability severity metrics; (8) Increase education and training tools; (9) Expand International Collaboration; (10) Enhance security and replace components of legacy software; (11) Advance public-private partnerships; and (12) Use formal methods.

KEY FINDINGS

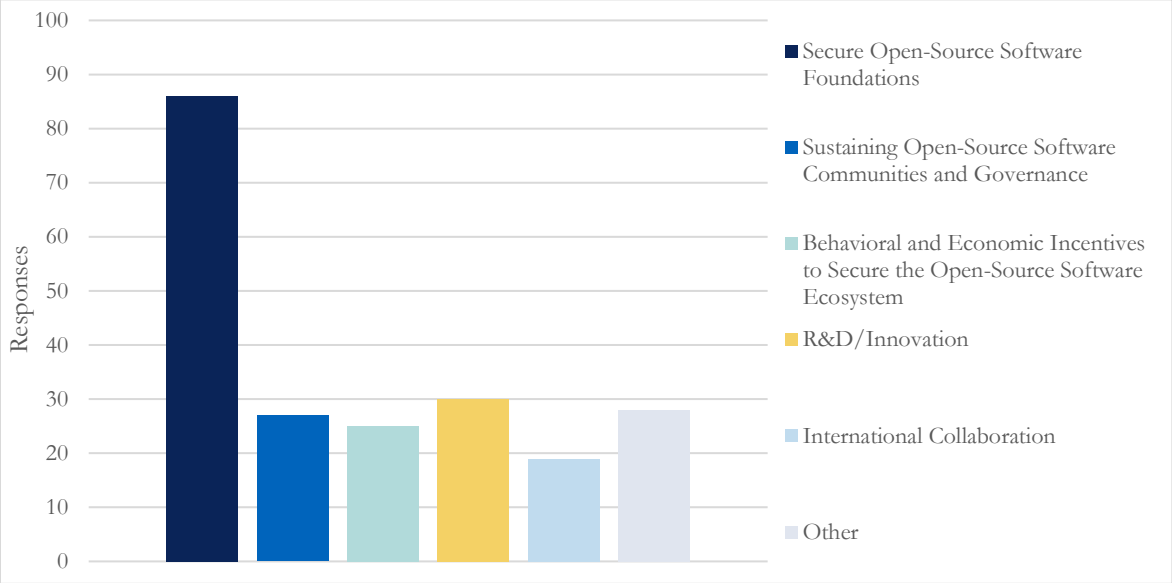

Chart 1.1 RFI Responses by Primary Area of Focus

Respondents provided submissions addressing five areas the Federal Government should aim to improve on in the security of the open-source software ecosystem. Respondents broadly agreed on the importance of increased adoption of memory-safe programming languages across the open-source software ecosystem. There was also consensus that implementing memory-safe programming would be significantly easier for new projects than for legacy projects. For the latter, many respondents supported using a tiered and prioritized approach as a way to optimize resources while focusing on the most critically important projects.

Adoption of memory-safe languages will also rely on a workforce that is versed in such programming, and respondents highlighted the need to invest in education across all levels of experience, from high school students to mid-career professionals. This investment will include education around memory-safe programming languages and contributing to open-source software projects. Respondents noted that given the size and importance of the open-source ecosystem, investments in all aspects of a safer ecosystem, from education to new projects to translation of existing libraries, will necessitate public-private collaboration.

Many respondents expressed the need for a strong Federal Government contributing role, working in conjunction with appropriate non-profit and private partners. Respondents also agreed on the need for improved coordinated vulnerability disclosure mechanisms to better inform open-source software developers of vulnerabilities. Respondents recommended other ways in which the Federal Government could play a stronger role in strengthening and securing the ecosystem, including greater participation in standards-setting bodies.

★ ★ ★ ★ ★ ★

Respondents also recognized that while characteristics of open-source projects have made them a source for innovation and progress, certain characteristics have also made them particularly susceptible to cyberattacks. As a way to counter this current state of affairs, respondents recommended that the Federal Government devise greater incentives to promote ecosystem safety and security, and improve the Federal Government's management of open-source software it consumes. This could include the creation of federal OSPOs at various agencies, and potentially a central Federal OSPO to coordinate activities among all federal OSPOs. Respondents also noted the ability of the Federal Government to significantly influence the transition to a safer open-source software ecosystem through the use of procurement rules and regulations that promote more secure development practices.

Respondents also largely agreed on the importance of making open-source software ecosystem safety and security an international effort, and recommended that the Federal Government work closely with international partner countries. In addition to working with partner countries to improve ecosystem security, the Federal Government can also learn from and potentially follow the lead of certain international efforts, including data security acts/regulations.

Finally, respondents advocated the Federal Government encourage and continue engaging with the open-source software community to foster the positive impact of open-source software across the economy, and to improve the security and resiliency of the entire ecosystem.

ANALYSIS

SECURE OPEN-SOURCE SOFTWARE FOUNDATIONS

Respondents provided widespread support for the use of memory-safe programming languages, particularly when developing new software projects. Respondents' preferences on how to encourage the use of memory-safe languages were more varied, with most endorsing voluntary adoption while several supported government-issued mandates.

Respondents provided several recommendations to address issues with legacy code in software programs. Many supported translation efforts – particularly those focused on critical projects – while others expressed concern about the resource-intensive nature of such efforts and suggested there would be a high likelihood of coding errors. Several suggested that automating legacy code translation into memory-safe code would create a more secure open-source software ecosystem, though they acknowledged that further research is necessary to achieve fully automated translation. This could include leveraging National and Department of Defense research laboratory initiatives (such as DARPA's Lifting Legacy Code to Safer Languages [LiLaC-SL] initiative).[v] Respondents further advised that translation efforts would need to include migrating firmware using memory-safe techniques.

Multiple respondents argued that code translations are unlikely to be undertaken by the private sector without some incentive. As the Apache Software Foundation stated, "memory-safety must be a goal, not an absolute requirement" and new memory-safe code/projects must be "supported by an active community that has the capacity and capability to maintain the rewritten code base."[vi]

Given the variety of programming languages in the open-source software landscape, respondents noted the importance of incentivizing the teaching of computer programming using memory-safe languages, both in academic settings and as part of workforce development and training. Of the respondents who highlighted specific memory-safe languages for emphasis in academic settings, most recommended Rust, while a few recommended Ada.

Under the sub-area "Strengthening the Software Supply Chain," respondents recommended standardizing SBOMs; Manifest Cyber stated this effort as a "bedrock requirement of software supply chain security." [vii] Further, they noted that efforts on this front could include supplying agencies with "SBOMs and attestation management tools that provide a high level of vulnerability database integration."[viii] Additionally, respondents noted that while current practice is that SBOMs are often created by analyzing the final binary or another software artifact, it is preferable to use tools that create SBOMs during the build process because build-time tools generally have access to more detailed and accurate information than what is available from analyzing an artifact.[ix]

Respondents additionally emphasized the need to secure open-source software infrastructure, such as package repositories used to distribute open-source software packages to developers. Some respondents recommended that the Federal Government help develop best practices for the security of package repositories,[x] and others suggested that the Federal Government fund non-

profits that operate open-source infrastructure, including package repositories, to ensure sustained security improvements.[xi]

Finally, to better protect end-users of open-source software, respondents recommended the Federal Government collaborate with the private sector to improve vulnerability data sources so producers in the supply chain are better informed of issues that require mitigation. Respondents also offered ideas about how to provide information on software vulnerabilities, with the Institute for Security and Technology suggesting the Federal Government create a "database of products known to contain vulnerable dependencies." [xii] Other respondents also noted the potential benefits of Vulnerability Exploitability eXchange (VEX) statements.[xiii] International collaboration on this endeavor was also recommended given the international nature of the open-source ecosystem.

SUSTAINING OPEN-SOURCE SOFTWARE COMMUNITIES AND GOVERNANCE

Many respondents supported a strong role for the Federal Government in helping to sustain open-source software communities, including through direct funding to open-source software foundations that support the ecosystem, investment in training, and centralization of Federal Government policies and best practices.

Respondents noted that many open-source software projects are maintained by individuals acting in a volunteer capacity and the lack of structural support for project maintenance increases the likelihood of project abandonment. Respondents argued that sustaining these projects requires a shift to a shared responsibility model, identification of the most critical open-source projects, and allocation of specific resources to support the highest priority projects. Additionally, respondents highlighted the need for funding to support professional training, sponsorships, and direct payments to independent open-source software developers.

Several respondents pointed to the German Sovereign Tech Fund as a model for the Federal Government with Dalewind Software and Consultancy stating "Emulating a similar path in the United States would be a significant step in the right direction" [xiv] Respondents also supported an expansion of the Open Technology Fund to improve the maintenance and security of the open-source software ecosystem. Some supported the idea of requirements or incentives for corporate entities that rely on and profit from open-source software to contribute resources to strengthening the ecosystem's security.

Finally, respondents called for improvements in federal agency management of their use of open-source software, with two respondents recommending an overarching federal OSPO to assist in such coordination. Respondents argued that a centralized federal OSPO could define government-wide policies related to open-source software, including identifying and driving best practices across agencies as needed.[xv]

BEHAVIORAL AND ECONOMIC INCENTIVES TO SECURE THE OPEN-SOURCE SOFTWARE ECOSYSTEM

Respondents suggested that to stimulate security in the open-source software ecosystem, the Federal Government should consider incentive models that include compensation, legal protections, and governance structures.

In the open-source software ecosystem, individual contributors to open-source software voluntarily support projects of their own choosing, unlike a traditional supply chain model where "suppliers" are tasked and compensated for their contributions. According to Tidelift, Inc., more than half of open-source software maintainers describe themselves as "unpaid hobbyists" who do not earn their income from sustaining open-source software projects.[xvi] Respondents stressed the importance of government funding to support libraries commonly used in critical infrastructure and incentivizing third-party analysis and validation. A respondent noted that effective funding for open-source software security improvements cannot be limited to identifying vulnerabilities, but must support remediating vulnerabilities as well.[xvii]

Relatedly, respondents pointed to the potential for financial incentives, including research and development tax credits, to encourage security improvements. The Open Source Security Foundation (OpenSSF) noted that "[f]urther guidance from the [Internal Revenue Service] on the availability of tax or payroll credits could encourage increased contribution (either through project funding or direct engineering efforts) to open-source software development and security enhancements."[xviii] Additionally, respondents recommended incentivizing government contractors to contribute back to open-source projects they depend on by favoring contractors who make contributions, whether financially or through code.[xix]

To assist private sector efforts, respondents suggested NIST, in collaboration with other government and industry partners, develop a Responsible Open-Source Software Consumption Framework to incorporate into NIST's Secure Software Development Framework.[xx] One respondent specifically noted the importance of modernizing the Federal Government's Vulnerabilities Equities Process, which is used to permit the government and its contractors to determine whether to disclose vulnerability information.[xxi]

Several proposals pointed to other incentives that include the creation of legal protections that prompt private entities to participate in open-source software security efforts. Proposed approaches include proactively creating a liability shield for entities providing security fixes upstream, and ensuring that any future software liability regime includes a safe harbor for open-source software maintainers and contributors, particularly those who participate as volunteers.

Other responses in this area focused on incentives to produce specific cybersecurity outcomes of national interest (e.g., code libraries, protocols, and the use of preferred frameworks, etc.). Similarly, establishing standards at the purchasing-level could help guide the ecosystem and avoid otherwise widespread effects. Establishing or leveraging public-private partnership models could aid in a standardization effort. Some respondents recommend the U.S. Government look to

international policies (e.g., Europe's Cyber Resilience Act or Product Liability Directive) for opportunities to coordinate efforts to address the growing threat environment.

RESEARCH & DEVELOPMENT/INNOVATION

There was broad support among commenters to apply evidence-based research to emerging technologies to advance knowledge and methods for securing open-source software. Specifically, some respondents noted that using ML and generative AI can identify persistent issues in the open-source software ecosystem, and that training generative AI tools could quickly remediate software vulnerabilities. However, respondents also noted that the use of AI without well-defined, proven best practices may yield insecure or imprecise results. Respondents recommended establishing best practices for development and the enactment of validation frameworks before using AI to assist with secure code creation, test creation, reviewer selection, and vulnerability remediation.

Respondents noted the possible use of LLMs to translate code into memory-safe languages but cautioned that verifying and validating AI-generated code would require significant human oversight at the outset with the expectation that the need for oversight would diminish over time.

To reduce classes of vulnerabilities, one respondent recommended NIST encourage the development of ML and LLM tools to identify emergent issues.[xxii] Another recommended NIST update NIST Interagency Report 8151 "Dramatically Reducing Software Vulnerabilities" on reducing classes of vulnerabilities.[xxiii] One submission suggested that CISA should publish guidance on specific ways to reduce classes of vulnerabilities in the open-source software ecosystem.[xxiv]

Many respondents commented on the need for an inventory of open-source software projects to inform software consumers about security risks associated with a given codebase. DeployHub, Inc. stated: "A federated, distributed evidence store . . . must consume and consolidate today's security insights across open-source software and private code bases."[xxv] Other respondents envisioned centralized software asset inventories, potentially including dependency information via SBOMs, at scales ranging from global to organization-specific.

Respondents also expressed the need for further research and development in several areas, including hardware security solutions; fuzzing; runtime security and security observability; methods of reducing classes of vulnerabilities; and automatic detection of and correction for common security vulnerabilities.

Finally, a number of respondents advocated for the use of formal methods/verification to improve the security and quality of open-source software components utilized in highly critical Federal Government projects. Wesley and Weston Pan emphasized that "open-source software components utilized in government funded projects be developed using formal methods."[xxvi] Respondents also stated that advances in formal methods have made them easier to use and that they are effective in identifying and addressing vulnerabilities in programming code before its release.

INTERNATIONAL COLLABORATION

In light of the global nature of open-source software, the majority of respondents expressed support for Federal Government engagement with international partners to advance joint priorities related to open-source software sustainability and security. Respondents further emphasized the need for harmonized international standards and regulations in pursuit of improved open-source ecosystem security. Respondents also stated the importance of coordination between private and public sector OSPOs, and the potential value of working with the European Union to learn from its experience with the General Data Protection Regulation, the Digital Services Act, and the Cyber Resilience Act.

OS3I ACTIONS IN 2024-2025

The Biden-Harris Administration aims to advance security in the development of advanced technologies, many of which use open-source software. President Biden's Invest in America Agenda ensures resources are available for next-generation innovations in software security. The Bipartisan Infrastructure Law provides incentives for investments in advanced cybersecurity technology.[xxvii]

Therefore, in alignment with the President's agenda, as established in the National Cybersecurity Strategy, and in support of the recommendations provided through the RFI, members of the OS3I have completed or plan to complete the following activities in 2024-2025:

1. Advance Research and Development

a. NSF is planning to launch an open-source software safety, security, and privacy track for the Pathways to Enable Open-Source Ecosystems (POSE) program, led by its new Directorate for Technology, Innovation and Partnerships (TIP), which was authorized by the CHIPS and Science Act of 2022.[xxviii] The program's goal is to transition open-source technologies into open-source ecosystems to further advance technologies and efficiently address national challenges while ensuring security and privacy.

b. The Department of Homeland Security Science and Technology Directorate and CISA initiated the Open-Source Software Prevalence Initiative.[xxix] This initiative, in line with CISA's Open-Source Software Security Roadmap, is designed to improve the national understanding of the distribution of use of open-source software components across critical infrastructure.

c. DARPA and the Advanced Research Projects Agency for Health (ARPA-H), in collaboration with top AI companies, are partnering on developing the Artificial Intelligence Cyber Challenge (AIxCC) — a two-year competition that brings together the best and brightest in AI and cybersecurity to safeguard software critical to all Americans.[xxx] AIxCC will ask competitors to design novel AI systems to secure this critical code and will award a cumulative $29.5 million in prizes to teams with the best systems, including $7 million in prizes to small businesses to empower entrepreneurial innovation during the initial phase of AIxCC.

d. A new DARPA program, Translating All C to Rust (TRACTOR) plans to build tools to help developers translate legacy software to achieve verifiably memory-safe Rust code, written with the same style and quality as a skilled Rust developer. TRACTOR tools, built with state-of-the-art programming language analysis and machine learning techniques, intend to accomplish this bulk transformation with a high degree of automation.[xxxi]

e. The Cyber Security and Information Assurance Interagency Working Group coordinates federal R&D to protect information, information systems, and people from cyber threats. This R&D supports the security and safety of information systems that underpin a vast array of capabilities and technologies used in many sectors of the U.S. economy and society. The cybersecurity R&D activities pursued by federal agencies are guided by the 2023 Federal Cybersecurity Research and Development Strategic Plan.[xxxii] The Strategic Plan already broadly supports many of the goals recommended within the RFI responses.

2. **Secure Package Repositories:** CISA, in partnership with the OpenSSF Securing Software Repositories Working Group, released the Principles for Package Repository Security framework, which establishes a voluntary security maturity model for package repositories, including actions such as requiring multi-factor authentication for packages.[xxxiii] At CISA's Open Source Software Security Summit, CISA announced actions that five of the most widely used package repositories are taking in line with the framework to secure entire ecosystems.[xxxiv]

3. **Partner with Open-Source Communities:** CISA, as identified in its Open Source Software Security Roadmap, is partnering with open-source communities to help improve the security of the open-source ecosystem operationally and strategically.[xxxv] CISA launched a collaboration channel to enable voluntary information sharing and collaboration with open-source software infrastructure operators.[xxxvi] This collaboration channel was leveraged to collaborate in real-time to respond to the XZ Utils compromise. Additionally, CISA held a tabletop exercise with open-source community members to test the response to an incident affecting an open-source library.[xxxvii]

4. **Promote further development and implementation of SBOMs:** CISA will continue work with stakeholders to identify and reduce gaps in SBOM scale and implementation. CISA has convened an international staff-level working group to discuss SBOMs. DARPA is further launching the Enhanced SBOM for Optimized Software Sustainment (E-BOSS) in an effort to mitigate vulnerabilities in dependencies.[xxxviii] Through the E-BOSS program, Enhanced Software Bill of Material (eSBOM) metadata technology enables rapid triage and remediation of vulnerabilities in software at scale. The toolchain components developed will emit advanced metadata alongside other SBOM information to effectively analyze and verify software.

5. **Strengthen the Software Supply Chain:** DHS S&T is partnering with CISA to fund and guide the development of multiple software supply chain visibility tools that can generate and integrate SBOMs with vulnerability information for use by both developers and system administrators. In FY24, this work resulted in the open-source SBOM translation tool, Protobom, which can translate SBOMs between the SPDX and CycloneDX standards.[xxxix] Protobom has been transferred to the OpenSSF to make this translation capability available to the global software security community.

★ ★ ★ ★ ★ ★

6. **Establish the First U.S. Government OSPO:** The Department of Health and Human Services (HHS) Center for Medicaid and Medicare Services (CMS) recently established the first Open-Source Program Office at a United States Federal Agency.[xl] The function of the OSPO is to establish and maintain guidance, policies, practices, and talent pipelines that advance equity, build trust, and amplify impact across CMS, HHS, and Federal Government's open-source ecosystem by working and sharing openly.

7. **Assign Vulnerability Severity Metrics:** The CHIPS and Science Act requires the Director of NIST to supply a qualitative measure of severity metrics to identify vulnerabilities with open-source software. NIST produces voluntary guidance to assist the entities maintaining open-source software repositories in the discovery and mitigation of vulnerabilities.[xli]

8. **Increase Education and Training Tools:** ONCD, together with its public and private sector partners, is leveraging Federal programs as part of a concerted approach to incorporate cyber content and skills across academic, occupational, and technical disciplines. In support of the National Cyber Workforce and Education Strategy, the Department of Labor made nearly $200 million available in grants to continue to support public-private partnerships that expand, diversify, and strengthen Registered Apprenticeships in information technology, supply chain, and other in-demand industries.[xlii] In June 2024, ONCD participated in the Cyber Across Disciplines conference in Chicago, Illinois. This event convened college and university faculty in cyber to encourage the integration of cybersecurity and secure programming practices across academic disciplines and industry sectors, as well as incorporating cybersecurity in computer science, AI, and emerging technology curricula.

9. **Expand International Collaboration:** The DHS and the European Union Commission have an ongoing Cyber Dialogue which meets in person once a year. As part of that effort, in December 2022 the collaboration added an open-source workstream that is led on the U.S. side jointly by the DHS Office of the Chief Information Officer and CISA.[xliii] Among other things, this international group continues to discuss possible policy changes, high-level guidance for both consumption and publication of open-source software, and common problems and solutions about open-source software security.

10. **Enhance Security and Replace Components of Legacy Software:** DARPA's Verified Security and Performance Enhancement of Large Legacy Software (V-SPELLS) program aims to create practical tools to help developers with legacy software modernization.[xliv] For example, many vulnerabilities in software occur where untrusted inputs, perhaps from the network, are initially being parsed and understood. V-SPELLS tools will aid developers in replacing hand-written parsing code with machine-generated parsers that are proven to be free of vulnerabilities. This work builds on another DARPA effort, Safe Documents, which produced robust parsing tools. Additionally, DARPA's Compartmentalization and Privilege Management (CPM) program is exploring ways to automatically transform legacy software into small code compartments, each with limited privilege, so that cyberattacks that exploit a vulnerability still can't compromise their ultimate target.

★ ★ ★ ★ ★ ★

11. **Advance Public-Private Partnerships:** CISA announced its Secure by Design Pledge which has, to date, received over 160 commitments from technology manufacturers to demonstrate measurable progress in building their products in a secure by design manner, including by reducing entire classes of vulnerabilities.[xlv]

12. **Use Formal Methods:** ONCD released a report titled "Back to the Building Blocks: A Path Toward Secure and Measurable Software" making the case that technology manufacturers can prevent entire classes of vulnerabilities from entering the digital ecosystem by adopting memory-safe programming languages, memory-safe hardware architecture, and formal methods.[xlvi] DARPA's Pipelined Reasoning of Verifiers Enabling Robust Systems (PROVERS) program is developing methods for traditional system and software engineers to secure software at scale by integrating formal methods techniques into standard toolchains and development practices. [xlvii] ONCD is also encouraging the research community to address the problem of software understanding and measurability to enable the development of better diagnostics that measure cybersecurity quality. ONCD is further encouraging the research community to address the problem of software understanding and measurability to enable the development of better diagnostics that measure cybersecurity quality.

CONCLUSION

Open-source software is ubiquitous and it underpins much of the hardware and software vital to America's national security and economic prosperity. The Biden-Harris Administration recognizes the unique value proposition of open-source software; when it is not secure and resilient, the resulting damage, disruption, and disorder is evident. Preventing and mitigating those risks cannot be accomplished by the Federal Government alone; it requires collaboration with the open-source software community.

The road toward this vision requires a recognition that America is at its best when we work together. Over the past year, the RFI process has made manifest the Administration's commitment to making policy with extensive input from those affected by it. Successful cyber policy demands it be written with the "end user" in mind and the OS3I carries this ethos in its work with the open-source software community.

Sustaining engagement with the ecosystem will not only continue the positive impact of open-source software across the economy, but improve the security and resilience of the nation. Together this partnership will champion a proactive cybersecurity posture and produce policies that minimize negative impact, maximize resilience, and ensure a prosperous and connected American future.

ENDNOTES

[i] Request for Information on Open-Source Software Security: Areas of Long-Term Focus and Prioritization, 88 Fed. Reg. 54315 (Oct. 9, 2023).
[ii] *The National Cybersecurity Strategy*, The White House, March 2023, *available at* National Cybersecurity Strategy | The White House.
[iii] The Cybersecurity Review Board, Review of the December 2021 Log4J Event, July 11 2022 available at: CSRB Report on Log4j. *See also* The Cybersecurity and Infrastructure Security Agency Blog on Lessons from XZ Utils: Achieving a More Sustainable Open Source Ecosystem available at: Lessons from XZ Utils.
[iv] *See* Fact Sheet, The White House, January 2024, *available at* Fact Sheet: Biden-Harris Administration Releases End of Year Report on OS3I.
[v] ONCD OSS RFI Responses [hereinafter Responses] Response from Datalytica, *available at* Regulations.gov.
[vi] Responses: Response from Apache Software Foundation, *available at* Regulations.gov.
[vii] Responses: Response from Manifest Cyber, *available at* Regulations.gov.
[viii] *Id*.
[ix] Responses: Response from Trail of Bits, *available at* Regulations.gov.
[x] Responses: Response from OpenSSF, *available at* Regulations.gov.
[xi] Responses: Responses from Rust Foundation, *available at* Regulations.gov and response from Python Software Foundation, *available at* Regulations.gov.
[xii] Responses: Response from Institute for Security and Technology, *available at* Regulations.gov.
[xiii] Responses: Responses from Secure Software Supply Chain Center, *available at* Regulations.gov; Apache Software Foundation, *supra* note vi; OpenSSF, *supra* note x.
[xiv] Responses: Response from Dalewind Software and Consultancy, available at Regulations.gov.
[xv] Responses: Responses from GitHub, *available at* Regulations.gov and Google, *available at* Regulations.gov.
[xvi] Responses: Response from Tidelift, *available at* Regulations.gov.
[xvii] Responses: Response from Apache Software Foundation, *supra* note vi.
[xviii] Responses: Response from OpenSSF, *supra* note x.
[xix] *Id*.
[xx] Responses: Response from Atlantic Council, *available at* Regulations.gov.
[xxi] Responses: Response from OpenSSF, *supra* note x.
[xxii] Responses: Response *available at* Regulations.gov.
[xxiii] Responses: Response from BSA/The Software Alliance, *available at* Regulations.gov.
[xxiv] Responses: Response from Trail of Bits, *supra* note ix.
[xxv] Responses: Response from DeployHub, *available at* Regulations.gov.
[xxvi] Responses: Response from Wesley and Weston Pan, Available at Regulations.gov.
[xxvii] *See* Investing in America - Build.gov | The White House.
[xxviii] National Science Foundation available at Pathways to Enable Open-Source Ecosystems (POSE) | NSF.
[xxix] DHS Science and Technology Directorate, *available at* Science and Technology Directorate | Homeland Security.
[xxx] Artificial Intelligence Cyber Challenge, *available at* AIxCC.
[xxxi] DARPA, Translating All C to Rust (TRACTOR), *available at* DARPA.MIL - Translating All C to Rust.
[xxxii] Executive Office of the President, National Science and Technology Council Report, "Federal Cybersecurity Research and Development Strategic Plan," December 2023, *available at* Federal Cybersecurity RD Strategic Plan 2023.
[xxxiii] DHS CISA Alert, *available at* CISA Partners With OpenSSF.
[xxxiv]DHS CISA Alert, *available at* CISA Announces New Efforts to Help Secure Open Source Ecosystem.
[xxxv] DHS CISA, *available at* CISA Open Source Software Security Roadmap.
[xxxvi] DHS CISA Alert, *supra* note xxxiv.
[xxxvii] DHS CISA, *available at* Open Source CTEP Situation Manual.
[xxxviii] DARPA Special Notice, *available at* E-BOSS Special Notice.
[xxxix] Press Release by OpenSSF, April 16, 2024, *available at* CISA, DHS S&T and OpenSSF Announce Global Launch of Software Supply Chain Open Source Project.
[xl] Centers for Medicare and Medicaid Services, *available at* CMS | Open Source Program Office.

★ ★ ★ ★ ★ ★

[xli] NIST Vulnerability Metrics, *available at* NVD - Vulnerability Metrics.
[xlii] *The National Cyber Workforce and Education Strategy*, The White House, July 2023, *available at* National Cyber Workforce and Education Strategy | The White House.
[xliii] DHS Joint Statement by United States Secretary of Homeland Security Mayorkas and European Union Commissioner for Internal Market Breton, January 26, 2023, *available at* Joint Statement by U.S. Secretary Mayorkas and EU Commissioner for Internal Market Breton.
[xliv] DARPA: V-SPELLS: Verified Security and Performance Enhancement of Large Legacy Software, *available at* DARPA.MIL - V-SPELLS.
[xlv] DHS CISA, *available at* Secure by Design Pledge | CISA.
[xlvi] *Back To The Building Blocks: A Path Toward Secure And Measurable Software*, The White House, February 2024, *available at* Back to the Building Blocks | The White House.
[xlvii] DARPA, available at Pipelined Reasoning of Verifiers Enabling Robust Systems (PROVERS).