October 9, 2023

Institute for Security and Technology (IST)
195 41st St. PO Box # 11045 Oakland, CA 94611
info@securityandtechnology.org
501(c)(3) organization

Submitted via email to OS3IRFI@ncd.eop.gov

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

To the 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:

The Institute for Security and Technology (IST) appreciates the opportunity to provide feedback on areas of long-term focus and prioritization for open-source software security. IST, a Bay Area-based non-profit, builds solutions to problems that arise at the nexus of emerging technologies and international security (please see the Appendix for more details on the organization).

In April 2023, IST's Open-Source Software Security Initiative published the seminal report "Castles Built on Sand," which put forward a series of recommendations towards securing the open-source software ecosystem. If adopted and implemented by stakeholders, we believe that these recommendations could help reduce the impact of vulnerabilities such as Log4j and prevent future vulnerabilities from arising.

We drew on insight derived from this research, as well as our breadth of experience across the cybersecurity and open-source communities, to respond to this request for information.

Contributors: Zoë Brammer, Silas Cutler, Marc Rogers, Megan Stifel

1. **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.**

Of the potential areas of focus outlined below, we recommend prioritizing securing open-source software foundations, sustaining open-source software communities and governance, and developing behavioral and economic incentives to secure the open-source software ecosystem.

- To begin **securing open-source software foundations**, we encourage:
    - Strengthening the software supply chain, specifically by incorporating automated tracking and updates of complex code dependencies, and designing tools to enable secure, privacy-preserving security attestations from software vendors, including their suppliers and open-source software maintainers. It is important that developers build these tools with automated identification of up-stream and down-stream integrity risks in mind.
    - The U.S. government should also create a database of products known to contain vulnerable dependencies. A number of private sector companies are working on similar projects, such as Sync's vulnerability database, but a central repository is critical to the government's ability to map the state of vulnerabilities in the open-source ecosystem and to begin to identify technical and policy solutions to reduce or eliminate these vulnerabilities and prevent their recurrence.
    - Further, the U.S. government could use artificial intelligence (AI) to identify vulnerabilities and other issues at scale to further illuminate the ecosystem. AI could also be leveraged to aid in making software documentation more accessible, and empower developer and consumer education.
    - We also advocate for reducing entire classes of vulnerabilities at scale, specifically by identifying methods to incentivize scalable monitoring and verification efforts of open-source software by voluntary communities and/or public-private partnerships. We encourage support for research into promising new methodologies to identify and monitor vulnerabilities, and the creation of tools to make these efforts more accessible and scalable. In particular, we encourage the U.S. government to marry this effort with aforementioned efforts to strengthen the software supply chain, including by developing parallel tools and approaches for finding vulnerabilities, and populating a database of known vulnerable software.
- Next, we encourage the U.S. government to focus on **sustaining open-source software communities and governance**.
    - In particular, we advocate for shifting open source software security to a shared responsibility model, and revisiting existing structures of liability around vulnerability management and mitigation.
    - Further, we commend the U.S. government for its stated goal of 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. This

maintenance and governance can draw from not only domestic expertise, but also the international cybersecurity community.

- Finally, we suggest that the U.S. government focus on **developing behavioral and economic incentives to secure the open-source software ecosystem**.
    - In particular, we encourage a focus on developing frameworks and models for software developer compensation that incentivize secure software development practices, and further incentivize and support secure operational practices within open-source projects. Achieving security by design and managing incidents requires operational skill sets in combination with software development talent.
    - We also encourage the U.S. government to assess applications of cybersecurity insurance and appropriately-tailored software liability as mechanisms to incentivize secure software development and operational environment practices.
    - Finally, we encourage the U.S. government to leverage federal procurement to incentivize secure software development, and encourage SBOM adoption at scale.

2. **What areas of focus are the most time-sensitive or should be developed first?**

We encourage the U.S. government to focus first on developing a centralized database of known vulnerabilities, along with tools and approaches to identify vulnerabilities at scale. It is critical to first understand the scale and scope of the open-source ecosystem and its associated security issues before identifying opportunities to increase its security.

We also encourage the U.S. government to reassess the incentive structure for those incorporating open-source code at scale in order to begin shifting the ecosystem toward a sustainable, shared, secure by design model.

At the same time, the U.S. government should continue to advance CISA's Principles and Approaches for Security-by-Design and -Default so that products coming to market do not compound the vulnerabilities identified through the first priority identified above.

3. **What technical, policy or economic challenges must the Government consider when implementing these solutions?**

The open-source community is composed largely of volunteer developers and corporate actors with overlapping and differing agendas. A key challenge in implementing solutions to secure the open-source software ecosystem will be ensuring solution design and implementation includes all stakeholders in the ecosystem. Identifying champions in the open-source community that can represent its views and empower them in identifying and implementing solutions is of critical importance to ensure solutions are both effective and feasible.

Further, different open-source stakeholders have differing agendas, which may complicate efforts to implement solutions. For example, our recommendation that the U.S. government create a centralized database of known vulnerabilities may be complicated by the fact that

companies are able to freely consume and adapt open-source code, making it difficult to track even known vulnerable code. For this reason, it is critical that the U.S. government reassess the economic incentive structure around leveraging open-source code such that corporate actors recognize that it is in their organization's best interest to ensure the security of open-source components in their products and services.

Actions to support or provide security to the ecosystem should be neutral in the agendas they work to uphold, and should center around the open-source community in order to ensure solutions are both effective and feasible.

4. **Which of the potential areas and sub-areas of focus described below should be applied to other domains? How might your policy solutions differ?**

Of the potential areas and sub-areas of focus described in this RFI, several are applicable to efforts to secure artificial intelligence at scale. First, strengthening the AI supply chain to ensure secure by design practices will be critical to maintaining the security of products and services as AI is integrated at scale. Designing tools to enable secure, privacy-preserving security attestations from AI vendors including their suppliers and maintainers will be an important step in the right direction. Further, identifying methods to incentivize scalable monitoring and verification efforts in the AI space by voluntary communities and/or public-private partnerships will become increasingly necessary to ensure the security of artificial intelligence.

Finally, a focus on shifting the economic incentive structure around AI development and proliferation should be a U.S. government priority. Existing market incentives allow developers to treat security as an afterthought, and encourage widespread proliferation of cutting edge technologies before a clear understanding of the associated risks can be developed and understood. Without re-assessing these incentive structures, it will be extremely difficult to ensure the security of products and services that integrate AI tools at scale.

Appendix

Organization Background

The Institute for Security and Technology (IST) builds solutions to problems that arise at the nexus of emerging technologies and international security. We are a unique, West Coast-based 501(c)(3) nonprofit that provides unparalleled access to technologists, policy makers, and civil society organizations that grapple with geopolitics, digital threats, and advanced computing. Our non-traditional approach has a bias for action, as we convene and build trust across domains, conduct applied research, and offer implementable solutions.

We divide our work into three thematic pillars:

1. Future of Digital Security. Societal-level dependence on digital technologies generates systemic security liabilities. We work to identify long-neglected vulnerabilities in modern digital infrastructure, and to propose ways to build security into software and hardware from the ground up.

   Projects include:
   - The Ransomware Task Force
   - The Open-Source Software Security Initiative
   - Applied Trust & Safety

2. Innovation and Catastrophic Risk. Despite the optimism about new technologies, some could or already do pose existential threats to society. IST searches for solutions to the risks introduced by technology, and strives to make technology itself a solution.

   Projects include:
   - Nuclear Crisis Control and Communications
   - Artificial Intelligence and Advanced Computing

3. Geopolitics of Technology. Emerging technologies can confer advantages and disrupt the international balance of power. As governments compete, they will shape innovation, supply chains, prosperity, and national and international security. IST takes on the implications of technology for global politics and security.

   Projects include:
   - Strategic Balancing Initiative

Highlighted Projects

The Ransomware Task Force:

One of the most well known examples of the success of our unconventional approach is the Ransomware Task Force (RTF). Using our unique, trusted ability to convene global leaders, IST undertook a 4 month sprint with both public and private partners in early 2021 to collaboratively develop a comprehensive framework to combat the scourge of ransomware. In April 2021, the RTF launched its seminal report, Combating Ransomware: A Comprehensive Framework for Action. The product of over 60 experts from industry, government, law enforcement, civil society, and international organizations, the report provided 48 specific recommendations and advocated for a unified, aggressive, comprehensive, public-private anti-ransomware campaign.

The framework developed by the RTF has led to Head of State-level interventions on ransomware, shaped legislation from the U.S. Congress, informed international governmental coalitions, and served as the basis for multiple national strategies for combating the national security risks posed by this virulent form of cybercrime. IST has continued to collect metrics and track progress against the threat, with numerous progress reports that can be found here.

Additionally, the work of the RTF has resulted in multiple ongoing work streams led by IST to actively combat the ransomware threat–resulting in multiple internationally recognized products for companies, civil society, and governments to use for action. These activities and products are detailed here. The combination of all of these efforts continues to result in more arrests, asset seizures, indictments, botnet takedowns, and disruptions of international criminal networks.

This impact shows IST's unique ability to conduct research, undertake collaborative and iterative analysis with global public and private sector leaders, and drive tangible, real-world impact with industry and government.

Open-Source Software Security Initiative:

Open-source software is the structural building block for the digital infrastructure that supports the modern world. At IST, we believe it is of the utmost importance to develop an approach that anticipates vulnerabilities and other risks such as malicious code before they impact the entire Internet infrastructure.

Our seminal report "Castles Built on Sand: Toward Securing the Open-Source Software Ecosystem," published in April 2023 with the generous support of Omidyar Network, proposed three lines of effort. First, shifting open-source software security to a shared responsibility model; second, redoubling support for existing secure software development frameworks, policies, and licenses; and third, reexamining approaches to vulnerability management and mitigation to ensure they account for open-source software.

The Open Source Software Initiative works to catalyze action towards more secure architectures, greater ecosystem resilience, and stronger policy postures—for the benefit of society across small businesses, individuals, open-source code developers, larger companies, academia, and the public sector.

Applied Trust and Safety:

As technology increasingly moderates our lives from enabling social discourse, facilitating economic participation, re-imagining the workforce, supporting supply chains to so much more, our collective future depends on appropriately managing the unique threats, vulnerabilities, and consequences attendant to digital services. Given technological diversity and threat evolution, organizations' Trust and Safety practices must evolve to include an adaptive and comprehensive framework.

IST seeks to address digital networks' trust and safety, including examining trust and safety normative frameworks and associated tools together with the policy and regulatory environments.

Team Biographies

The project was conducted with the following core team and advisors:

- Zoë Brammer, Cyber and Information Operations Associate, Researcher
- Silas Cutler, Adjunct Senior Cyber Threat Advisor, Project Consultant
- Marc Rogers, Adjunct Senior Technical Advisor, Project Consultant
- Megan Stifel, Chief Strategy Officer, Project Policy Lead

Zoë Brammer is the lead researcher for the Institute for Security and Technology's Ransomware Task Force and manages projects and research development on open source software security and open source artificial intelligence. Her portfolio focuses on a range of topics where cybersecurity practices and the cyber threat landscape intersect with government and economic policy, including research on digital systems and democracy, the future of digital security, ransomware, cryptocurrency, open source software security, and artificial intelligence.

Zoë holds BAs in International Relations and Economics from Clark University, and completed the General Course at the London School of Economics. She has had her work published in Tech Policy Press, Dark Reading, "Security and Society in the Information Age", Inkstick Media, and on the NatSpecs Blog.

Silas Cutler is an experienced security researcher and malware analyst. His focus has been researching organized cybercrime groups and state-sponsored attacks.

Marc Rogers is Co-Founder and Chief Technology Officer for the AI observability startup nbhd.ai. Marc served as VP of Cybersecurity Strategy for Okta, Head of Security for Cloudflare and Principal Security researcher for Lookout. He's been a CISO in South Korea and spent a decade managing security for the UK operator, Vodafone. In 2012, Marc co-founded the disruptive Bay Area security startup "Vectra".

Marc's core expertise is as a security researcher and whitehat hacker. Notable examples of his research include his hacks of Apple's TouchID, Google's Glass and automotive hacks such as that of the Tesla Model S.

Marc uses this expertise in his roles as an Adjunct Senior Technical Advisor for IST, a member of the Ransomware Taskforce, and co-founder of the CTI League. For his work in the CTI League Marc was nominated as one of Wired Magazine's people making things better in 2020. Last, Marc's an organizer and the Head of Security for DEF CON.

Megan Stifel is the Chief Strategy Officer at the Institute for Security and Technology, where she helps lead the organization's work under the Future of Digital Security pillar, including serving as Executive Director of the Ransomware Task Force. Megan previously served as Global Policy Officer at the Global Cyber Alliance and as the Cybersecurity Policy Director at Public Knowledge. She is a Visiting Fellow at the National Security Institute. Megan's prior government experience includes serving as a Director for International Cyber Policy at the National Security Council. Prior to the NSC, Ms. Stifel served in the U.S. Department of Justice as Director for Cyber Policy in the National Security Division and as counsel in the Criminal Division's Computer Crime and Intellectual Property Section. Before law school, Ms. Stifel worked for the U.S. House of Representatives Permanent Select Committee on Intelligence. She received a Juris Doctorate from Indiana University and a Bachelor of Arts, magna cum laude, from the University of Notre Dame. She is a member of the Aspen Global Leadership Network as a Liberty Fellow.

Megan has testified before Congress; been featured on NPR, BBC, and the PBS NewsHour; published in *The Hill* and *VentureBeat*; and quoted in the *Washington Post*, *The Wall Street Journal*, *Rolling Stone*, and *Politico*, among other publications.