The Software Alliance

BSA

Kemba E. Walden
National Cyber Director, Acting
The White House
1600 Pennsylvania Avenue NW
Washington, DC 20500

Via regulations.gov

November 8, 2023

Ms. Walden:

BSA | The Software Alliance[1] appreciates your office's active engagement with stakeholders on the open-source software security. BSA supported both the development of the US National Cybersecurity Strategy and its Implementation Plan. We believe that partnership between governments and industry is the most direct path toward a more secure future.

BSA is the leading advocate for the enterprise technology sector. Our members are among the world's most innovative companies and help to drive digital transformation by providing the solutions that make businesses and government agencies more competitive and effective, including cybersecurity; identity, credentialing, and access management; human resources management; customer relationship management; design and modeling; collaboration and communication; data analytics, visualization, and backup; and ticketing and workflow solutions.

BSA recently published our 2024 Global Cyber Agenda, which represents the enterprise technology sector's cybersecurity priorities. It urges policymakers to build on a successful foundation of public-private partnerships, risk-based approaches, and internationally recognized standards and best practices. It identifies software security as a top priority. Like the Office of the National Cyber Director (ONCD), BSA recognizes that open-sources software plays a vital role in modern life and produces immense benefits to businesses,

[1] Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Okta, Oracle, Palo Alto Networks, Prokon, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

government agencies, customers, and citizens. We also appreciate that that the cybersecurity community should work to improve the security of open-source software – and in fact, already is.

BSA has called on both the private and public sectors to improve the security of their own software and the security of broader digital ecosystem. To that end, BSA offered twelve aggressive but achievable recommendations that would minimize vulnerabilities in open-source software, improve the process for identifying vulnerabilities and developing patches, and expedite the distribution and implementation of patches. You can find these 12 recommendations here: BSA Recommendations for Open Source Software Security.

In addition to these twelve recommendations, BSA offers the following comments.

I. Sub-area: Fostering the adoption of memory safe programming languages.

BSA agrees that adopting memory safe programming languages presents one opportunity to improve software security, including open-source software security. However, organizations must move to memory safe programming languages thoughtfully otherwise they may address one risk while creating another. Additionally, spending resources on migrating to a memory safe language may not be the best use of limited cybersecurity resources. Despite these and other challenges, stakeholders should not unreasonably delay the use of or transition to memory safe programming languages.

Policymakers should appreciate that some hardware may not be capable of using different programming languages, and today, the hope of artificial intelligence completing the bulk of the transition, while worth exploring, is not feasible. Ultimately, the most important outcome is more secure software, whether that arises from memory safety, or other opportunities to improve software security.

BSA suggests governments around the world should support, government agencies should lead, and software producers should implement a policy of “strategic adoption.” Strategic adoption requires active risk management of memory safety, invests in research and development, and prioritizes new code. For more information about the policy of strategic adoption see Memory Safety: A Call for Strategic Adoption.

II. Sub-Area: Reducing entire classes of vulnerabilities at scale

BSA supports ONCD efforts to work with industry to address entire classes of vulnerabilities, for example, by leveraging the policy of strategic adoption to address vulnerabilities related to memory safety (see above).

BSA suggests that ONCD’s efforts to reduce entire classes of vulnerabilities begin with government and industry collaborating to determine what class of vulnerabilities presents the greatest opportunity to improve cybersecurity. One opportunity to collaborate is revisiting the National Institute of Standards and Technology’s (NIST) NISTIR 8151, Dramatically Reducing Software Vulnerabilities, to determine whether its findings remain accurate and should be acted upon, or whether NIST and industry should collaborate to update the document.

III. Sub-Area: Strengthening the software supply chain

Cybersecurity supply chain risk management and software supply chain risk management are complex challenges that defy simple solutions. One of the many reasons for this complexity is that modern software is frequently updated; of course, ONCD should encourage frequent updates because they improve functionality and security.

There are multiple ways ONCD can meaningfully help industry strengthen software supply chains. Two of which we discuss in greater detail in other sections: implementing the policy of strategic adoption (above) and requiring colleges and universities to provide appropriate instruction on secure development (below). Other opportunities include:

- Rationalizing US Government efforts on supply chain security. Today, there are multiple efforts related to supply chain security, including software security. Clarifying how these efforts do or do not relate, when and how industry can engage in these efforts, and what US Government agency is leading would enhance these efforts.
- Encouraging the development and use of AI systems to improve the secure development of software, including through actions identified in the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. At the very least, this effort should ensure that laws and policies that generally address AI explicitly carve out the use of AI for cybersecurity and software security purposes.
- Supporting ongoing efforts to ensure that software bills of materials (SBOMs) provide concrete improvements to cybersecurity. BSA supports the development and use of SBOMs to expedite incident response. We caution that the cybersecurity community has not yet sufficiently defined or standardized SBOMs. Consequently, the requirement of SBOMs, for example, in the context of contracts with the US Government, is premature. Additionally, even when SBOMs are ready, they will not be a panacea.
- Requiring software producers to maintain a coordinated vulnerability disclosure (CVD) program, which they should do using internationally recognized standards like ISO/IEC 30111 and 29147. CVD programs promote a responsible, risk-based approach to vulnerability disclosure.
- Leveraging existing authorities designed to secure the information and communications technology supply chains, such as implementing requirements that defense vendors disclose whether source code has been shared with countries of concern.

IV. Sub-Area: Developer education

The National Cybersecurity Strategy accurately notes that “even the most advanced software security programs cannot prevent all vulnerabilities.” Even as we accept that no set of software development practices can prevent all vulnerabilities, enterprise technology companies are working to reduce errors, including through strong developer education and training.

As the National Security Telecommunications Advisory Committee (NSTAC) report on Software Assurance in the Information and Communication Technology and Services Supply Chain notes, software developers need to know how to keep code largely free of coding errors. BSA suggests ONCD work to require colleges and universities that provide instruction on software development, to include in their curriculum appropriate instruction on secure software development processes, secure capabilities, and secure lifecycle management. Further, these colleges and universities should, at a minimum, introduce students to best practices for secure software development like those in the BSA Framework for Secure Software.

Further, BSA suggests ONCD work with industry to design incentives for workers to improve secure software development specifically and cybersecurity risk management in general.

V. Area: Sustaining Open-Source Software Communities and Governance

The most direct step the US Government can take to sustain open-source software communities is engaging in the development and maintenance of the open-source software on which its departments and agencies rely. To be successful, this effort must begin with a long-term commitment and likely requires US Government agencies to provide their employees and contractors with the time and other resources necessary to participate in these activities. This investment will be well worth it.

Further, ONCD should encourage international partners to commit to the same long-term and meaningful efforts to develop and maintain open-source software.

VI. Area: R&D/Innovation

Enterprise software companies are already using AI during the software development process to detect and address vulnerable code. However, efforts to regulate AI risk undermining the use of AI for this, and other similar software security and cybersecurity purposes.

The US Government should promote the use of AI to bolster cybersecurity generally, and secure software development specifically. The US Government should limit efforts to regulate AI systems to high-risk uses and not impede the use of AI to improve cybersecurity. For more information about how the US Government can advance these efforts see: AI for Cybersecurity: Ensuring Cyber Defenders Can Leverage AI to Protect Customers and Citizens.

VII. Area: International Collaboration

The open-source software ecosystem, by its nature, knows no borders. Therefore, taking a country-based approach to issues within the open-source software community is unlikely to be successful and any efforts that result in a balkanized open-source software ecosystem would undermine the security and functionality of this important ecosystem.

However, ONCD can, and should, engage international partners in its pursuit of more secure open-source software. This engagement should aim to build support for governments:

- Participating in and funding the development and maintenance of open-source software projects
- Ensuring efforts to regulate AI do not impact the use of AI for cybersecurity generally or secure software development specifically.
- Requiring educational institutions to provide appropriate instruction on secure software development processes, secure capabilities, and secure lifecycle management.
- Participating in the development and implementation of internationally recognized standards used to improve secure software development.

This engagement should include a long-term commitment of technical experts housed in organizations like the Cybersecurity and Infrastructure Security Agency and National Institute of Standards and Technology. It should focus on developing code with fewer vulnerabilities, maintaining that software, and addressing vulnerabilities.

Most importantly, ONCD's international engagement should consistently involve industry. While BSA recognizes that some conversations must be solely between governments, the nature of open-source software security dictates that most of the conversations ONCD has with international partners would benefit if they also include industry perspectives.

VIII. Moving Forward

The enterprise software industry is committed to working with the US Government and other governments around the world to better secure open-source software and ensure it can continue benefit all people. BSA appreciates ONCD's engagement on this issue and looks forward to working together to ensure a secure and resilient open-source software ecosystem.

Respectfully,

Henry Young
Director, Policy