February 20, 2024

SIIA Response to CISA Request for Information

Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software

On behalf of the Software & Information Industry Association (SIIA), we write in response to the request for information issued by the Cybersecurity and Infrastructure Security Agency (CISA) regarding the white paper, "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software."[1] SIIA supports the overall goals of the white paper. As CISA considers guidance to support more robust secure-by-design, we encourage the agency to focus on design frameworks and stakeholder input, establishing long-term principles, and specific areas where the government can help advance the development of secure-by-design systems.

SIIA is a trade association representing roughly 375 companies reflecting the broad and diverse landscape of digital content providers and users in academic publishing, education technology, and financial information; creators of software and platforms used by millions worldwide; and companies specializing in data analytics and information services. Our mission is to protect the three prongs of a healthy information environment essential to that business: creation, dissemination and productive use.

1. **CISA should conform future guidance to the NIST Secure Software Development Framework. *(Response to questions 3b, 4a, 5a, 7a, 7b)***

SIIA strongly supports the overall aims of the white paper. Simplifying cybersecurity via secure-by-design philosophy and implementing this across the software development lifecycle (SDLC), especially at the early stages of software manufacturing, is critical. Secure-by-design principles must be a focal point of effective software development. Monitoring and "owning" customer security outcomes, increasing accountability and transparency throughout the early design process, and prioritizing secure-by-design manufacturing at an organizational level are each laudable goals.

At the same time, we believe greater alignment with the NIST Secure Software Development Framework (SSDF) and increased stakeholder engagement, particularly with domestic businesses, would better accomplish these goals.[2] We recommend that CISA hew close to the framework articulated in NIST's SSDF in order to advance secure-by-design across the public and private sectors. The SSDF was the product of widespread stakeholder

[1] Secure By Design (cisa.gov); Federal Register :: Request for Information on "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software".
[2] Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities (nist.gov).

consultation. It represents a framework of best practices that have already been adopted by many U.S.-based firms. Divergent guidance may not mesh with the cybersecurity strategies of even the most technologically advanced entities. We believe it would be counterproductive to introduce disparate and competing principles to this framework, let alone new specific controls.

In addition, as CISA proceeds towards advancing secure-by-design, we encourage the agency to actively seek feedback from multi-stakeholder organizations, particularly industry-led organizations, as much as possible. In the past and during the drafting of this white paper, the agency emphasized collaboration with foreign governments endeavoring to implement secure-by-design philosophy in their own countries. However, many of the questions posed in this RFI—including queries related to costs incurred during implementation, vulnerabilities to manufacturers, and field studies—require feedback from the private sector. Taking advantage of domestic industry expertise is a unique strength given U.S. leadership in secure-by-design technology, and one we believe CISA should lean on as it moves forward in this area.

2. **Principles rather than rigid requirements will advance adoption of secure-by-design software.** ***(Response to questions 3a, 3c, 5a(ii), 6b and c, 10b)***

SIIA supports the adoption of flexible principles that are adaptable to changes in technology and cybersecurity priorities, and caution against rigid controls that may be obsolete in even the near or medium term.

Focusing on individual mechanisms and controls fails to imagine the array of security threats that will materialize post-implementation, as well as the priorities and needs of public and private entities responding to these threats. The more specific and rigid the requirements are, the more likely they will simply cement legacy controls at the expense of advances in secure-by-design technology. They would also prevent this guidance, no matter how germane to current security challenges, from remaining relevant through the years and serving as a useful reference point for well-intentioned manufacturers and developers of the technology.

We encourage CISA to consult with industry groups on any proposed specific controls in the interest of both future proofing the guidance's relevance and aligning it with existing best practices at a high level.

3. **The government should actively support standardization of secure-by-design technologies.** ***(Response to questions 1a and 3b)***

SIIA believes the government has several critical roles to play in both encouraging and pushing the boundaries of secure-by-design software and technological development.

First, CISA should promote the adoption of security best practices "up front" in the development process. Of course, this simplifies and standardizes the implementation of secure technology – yet it is also where mistakes will likely have lasting consequences.

Research into best practices on the part of CISA and other agencies is thus critical. Through white papers such as this one, the U.S. government has the opportunity to set

adaptable standards for foundational software development and principles that can be implemented early in the SDLC. In concert with the developer ecosystem, getting this right promises to dramatically improve cybersecurity protections writ large. Of course, this is also why principles instead of specific controls are most helpful. For example, memory safe languages promise to significantly aid cybersecurity protections. Yet these are controls, not principles, and therefore should not be built into a standardized framework or secure-by-design protocols for early software development.

We also recommend that CISA include a review of recurring vulnerabilities as a routine part of any vendor acquisitions. This will promote an understanding of the effectiveness of its stated principles, as well as providing the agency with a window into how new developments are affecting secure-by-design goals. In addition, it will address the real problem of private entities attesting to protections they cannot guarantee, which occurs frequently when performance vulnerabilities are left unexamined. SIIA believes testing for vulnerabilities is a crucial frontier for secure-by-design development, and would go further to suggest it should even play a role in procurement. If the U.S. government purchases software that conforms to adoption of its principles and effectively verifies compliance, these principles are that much more likely to be adopted and improve security outcomes as a result.

* * *

SIIA strongly supports the objectives of this white paper. At the same time, we caution CISA to lean on the SSDF as well as feedback from the private sector, build out principles over prescriptive requirements, and empower the government to incentivize and promote secure-by-design software development at the outset of development as well as on an ongoing basis.

Respectfully submitted,

Paul Lekas
Senior Vice President and Head of Global Public Policy and Government Affairs

Anton van Seventer
Counsel, Privacy and Data Policy

Software & Information Industry Association