Comments of the Coalition to Reduce Cyber Risk (CR2) to the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security (DHS)

February 12, 2024

WC Docket No. CISA–2023–0027

Re: Request for Information on ''Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software''

The Coalition to Reduce Cyber Risk (CR2) submits this comment in response to CISA's request for information (RFI) on its whitepaper, "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software."[1]

Our members represent global organizations from numerous sectors, including IT, financial services, and communications, that are committed to security, trust, and economic growth and opportunity. Our members have deep expertise in cybersecurity and enterprise risk management, as well as unique insights into cross-sector independences and global interconnectivity, which drive the need for consistent, foundational approaches to cybersecurity risk management across sectors and geographies. As such, we have set out to work collaboratively with public and private sector entities to improve cybersecurity risk management practices that will both enhance cybersecurity and support economic growth.

Our comments will provide feedback on the following areas:

- International Collaboration
- Secure Software Development Framework (SSDF) & International Standards

[1] Department of Homeland Security (DHS), Request for Information on ''Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software''

International Collaboration

CR2 would like to commend CISA on its ability to garner international support and sign-on for the most recent version of its white paper on secure software development principles. We underscore the importance of prioritizing continued international collaboration between CISA and international stakeholders on secure-by-design efforts, to ensure greater global alignment and the more seamless implementation of security best practices across borders.

We are concerned, however, with the lack of formal industry engagement during the development of the *Principles*, which led to the development of an approach which does not reflect industry-supported frameworks such as NIST's Secure Software Development Framework (SSDF). Nor is it clear how input provided through this consultation can be incorporated by the U.S. Government without the agreement and endorsement by all signatories to the original document.

We support CISA's work to update and implement the Secure by Design Principles and identify ways for our international partners to incorporate the guidance into their domestic policies. Conducting a mapping exercise of all the entities that have implemented the secure-by-design principles, and identifying best practices and lessons learned across the signatories, would also be an invaluable resource to industry in this regard.

Each of these initiatives should be done, however, with robust stakeholder engagement into the process both to enhance the practicality of the principles themselves and to ensure multi-stakeholder buy-in to the initiative.

Secure Software Development Framework (SSDF) & International Standards

A key priority of CR2 is to promote greater adoption of globally aligned international standards. We point to the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF) as a powerful cybersecurity risk management framework.

The CSF has gained widespread international adoption by both industry and governments, in part because it is mapped to widely-utilized international standards.[2]

In much the same way, NIST's Secure Software Development Framework (SSDF) uses international standards such as IEC 62443: Security for Industrial Automation and Control systems; ISO 27034: Security Techniques, Application Security; and ISO 29147: Security Techniques, Vulnerability Handling Processes as key references.[3] Moreover, the SSDF was developed with robust industry participation, and is intended to be iterative to reflect lessons learned and feedback from implementation.

We recommend that CISA use the SSDF to inform their Secure-by-Design initiative. By basing the effort on a framework that is rooted in international standards, that has already received in-depth feedback, and is already utilized by industry, CISA will leverage a widely-utilized, industry-supported framework rather than layering an additional and potentially duplicative reference point on industry partners.

* * *

CR2 appreciates the willingness of CISA to seek feedback from industry stakeholders through this public consultation, and we hope this response will be helpful to CISA as they continue their work on the Secure-by-Design initiative.

Respectfully Submitted,

Coalition to Reduce Cyber Risk

CC:

Alex Botting, Venable LLP

---

[2] National Institute of Standards and Technology (NIST), Cybersecurity Framework, https://www.nist.gov/cyberframework/framework, (last accessed Fe. 6, 2024).

[3] NIST, SP 800-218, Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities, Feb. 2022, https://csrc.nist.gov/pubs/sp/800/218/final.