February 20, 2024

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
245 Murray Lane
Washington, District of Columbia 20528

RE: Comments of ACT | The App Association to the Department of Homeland Security Cybersecurity and Infrastructure Security Agency on *Request for Information on "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software"* (88 FR 88104)

Dear Director Easterly:

ACT | The App Association writes to provide input to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) on its white paper, "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software."[1]

The App Association is a global trade association for small and medium-sized technology companies. Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology. Today, the value of the ecosystem the App Association represents–which we call the app economy–is approximately $1.8 trillion and is responsible for 6.1 million American jobs, while serving as a key driver of the $8 trillion internet of things (IoT) revolution.[2] We applaud CISA's efforts to advance security by design and a secure software development lifecycle (SDLC), and to provide guidance to organizations to better understand, manage, reduce, and communicate cybersecurity risk across emerging technology areas.

App Association small business members, who typically do not have multiple product lines to distribute organizational risk across, are dedicated to security by design and security by default, and we agree that the integration of product security is a critical prerequisite to features and speed to market. Indeed, security by design is a priority driven by the market today as much as compliance with laws and regulations, which is why our community goes far above and beyond legal requirements to proactively ensure security from the earliest phases of design and development.

With fewer resources than larger entities, App Association small business members benefit from guidance and assistance in cybersecurity threat risk mitigation. Along with other federal leaders such as the National Institute of Standards and Technology (NIST), CISA should continue to

[1] https://www.nist.gov/news-events/news/2023/08/nist-drafts-major-update-its-widely-used-cybersecurity-framework

[2] https://actonline.org/thebackboneofamericaninnovation/.

serve as a leader and coordinator within the U.S. government in guiding the management of cybersecurity risk across sectors. We appreciate that CISA, like NIST, embraces a scalable cybersecurity risk management approach that enables developers to adjust their cybersecurity risk management tactics to anticipated harms/intended uses and the unique circumstances in play for that product or deployment. **The App Association broadly applauds CISA's security by design and SDLC recommendations in its white paper and is committed to advancing the security by design/default mindset across the software development ecosystem.**

Building on the above, the App Association offers the following further specific inputs and recommendations:

- ***Clarified scope and "living" nature of CISA's recommendations:*** We appreciate CISA's clarifying text addressing the applicability of its recommendations to emerging technologies such as artificial intelligence (AI). We agree that security by design concepts should underlie the development of cutting-edge technologies just as they do for existing categories and verticals of software. We also appreciate CISA's commitment to continue to take in input on use cases where its security by design guidance may not map well to a use case, which may lead to updates to CISA's guidance.
- ***Operationalizing CISA's security by design concepts and recommendations:*** With a unified approach committed to security by design now established across government and the private sector, the most difficult part remains ahead: implementation. It will certainly be difficult to integrate security by design curriculum into the software development ecosystem. It will be harder still to ensure that enterprise buyers are appropriately articulating security by design requirements through their requests for proposals using the correct benchmarks. CISA's recommendations, coupled with leading industry standards and practices, will require a public-private partnership supported by federal funding to accomplish both. Such a public-private partnership must build on, among others, the critical infrastructure cybersecurity partnership in place today (e.g., the IT Sector Coordinating Council[3]).

  The App Association is committed to evangelizing security by design practices to its small business innovator community and others, and to work with CISA, NIST, and others to realize a software ecosystem that is secure by default. To realize shared security by design goals, a focus on small business education and resources will be required, and we encourage CISA's support for small business cybersecurity risk management improvements through focused outreach and education, the development of further small business-focused resources, and grants and other means of support for small business implementation of the recommendations in CISA's white paper. The App Association commits to assist CISA in its small business support across these, and other, means, and welcomes the opportunity for further collaboration moving forward.

  Further, CISA should publish aggregate security-relevant statistics and trends on a recurring basis (annual or more frequently) that will support alignment with security by design best practices it recommends. Examples of areas where data insights and best practices/examples could help support CISA's security by design goals include multi-factor authentication adoption and continued use of unsafe legacy protocols, patching statistics and best practices (e.g., what percentage of customers are on the latest version of leading products and what is being done to make updates easier and more

[3] https://www.it-scc.org/.

reliable), and data on unused principles (aggregate information on excessive permissions across customer bases as well as the nudges and other changes to products being made to reduce customers' attack surfaces.

- ***International coordination:*** The App Association appreciates CISA's collaboration with the many security agencies and multinational fora noted in the white paper. International alignment on security by design policy is vital to a secure global digital economy and eases trade barriers.

The App Association appreciates the opportunity to provide this input to CISA and looks forward to continued collaboration to advance security by design across the software ecosystem.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005
p: +1 517-507-1446
e: bscarpelli@actonline.org