February 20, 2024

Megan Doscher
Branch Chief, Security at Scale
Cybersecurity and Infrastructure Security Agency

Via regulations.gov

Dear Ms. Doscher:

BSA | The Software Alliance[1] appreciates the opportunity to respond to the Cybersecurity and Infrastructure Security Agency's Request for Information on Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software (Shifting the Balance).

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's 2024 Global Cyber Agenda identifies improving software security as a top priority, which continues BSA's commitment to driving policies and identifying best practices to improve software security. One example of these efforts is BSA's Framework for Secure Software, which contains the organizational processes and product security capabilities that combine to improve software security, and which the National Institute of Standards and Technology (NIST) cites frequently in its Secure Software Development Framework (SSDF).

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

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

Shifting the Balance contains many valuable ideas, which include, but are not limited to calls to:

- Eliminate default passwords, though notably it is a common and reasonable practice to ship devices with default passwords that a user must change upon first use;
- Discourage the use of unsafe legacy products;
- Prioritize the use of memory safe languages, as BSA advocated in Memory Safety: A Call for Strategic Adoption; and
- Establish vulnerability disclosure programs.

Nonetheless, we see opportunities to improve the document, and provide the following comments in the hopes that future drafts incorporate the views of industry partners.

## I. Opportunities To Improve Processes and Coordinate Across Government

As noted in BSA's 2024 Global Cyber Agenda, the most effective path toward improved cybersecurity is collaboration between industry and government. BSA urges CISA to engage with industry partners as early in the process as possible to enable all stakeholders to refine the concepts in these documents and prepare to make them a reality.

The entire US Government should have, and communicate clearly to stakeholders, a holistic, whole-of-government approach to both cybersecurity generally and software security specifically. CISA's work should clearly align with these efforts. We are supportive of the US National Cybersecurity Strategy and its Implementation Plan. However, it is unclear how the efforts of CISA and other US Government agencies fit together, and the most effective ways industry partners can engage on these efforts. For example, in addition to responding to Shifting the Balance, open efforts include:

- CISA's efforts to finalize the regulations implementing the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), finalize the Secure Software Attestation Common Form (Common Form), and obtain pledges from software producers to take specific steps identified in Shifting the Balance, as well as CISA's work on Software Bills of Materials (SBOMs).
- The Office of the National Cyber Director's efforts following on its requests for information on both open-source software security and cybersecurity regulatory harmonization.
- The General Services Administration's (GSA) recent Notice of Proposed Rule Making (NPRM) on Cyber Threat and Incident Reporting and Information Sharing.
- The Department of Homeland Security's efforts following on the publication of its September 2023 report Harmonization of Cyber Incident Reporting to the Federal Government.
- NIST's efforts to update the Cybersecurity Framework.
- The National Security Council's efforts on trusted technology.

To increase the likelihood that these efforts are successful, they should be coordinated and proceed sequentially, completing a first activity that forms an input for a second activity before beginning that second activity. Problematically, for example, GSA's NPRM proposes requirements for incident reporting before CISA has finalized its regulations implementing CIRCIA and CISA is exploring seeking pledges from software producers based on Shifting the Balance, while it is simultaneously seeking feedback on the substance of the document and before it has finalized the Common Form.

BSA recommends CISA generally proceed sequentially, and specifically improve Shifting the Balance and address BSA's Response to CISA's Request for Comments on CISA's Secure Software Development Attestation Common Form before considering seeking pledges from software producers.

## II. Principle 1: Take Ownership of Customer Security Outcomes

### A. Recognize Customers Have Security Responsibilities

The document suggests that software producers "take ownership of customer security outcomes."

Numerous adverse security outcomes arise from causes far outside the reach of a software producer. Some of those outcomes arise from advanced persistent threats funded by nation-states which are outside the reach of both software producers and law enforcement agencies. Other outcomes arise from more mundane threats within a customer's own organization, like insider threats or poor internal security practices. In short, there are many incidents for which a software producer has exceedingly limited or potentially no ability to impact.

Unfortunately, Shifting the Balance communicates to customers that security is no longer their responsibility and in so doing, harms the cause of cybersecurity more than it helps it. While there are opportunities for software producers to bear more responsibility, Shifting the Balance goes far past what a software producer could reasonably, and in some cases possibly, be expected to bear. As a matter of both process and substance, CISA should not undermine the accepted shared-responsibility approach without a deep and transparent discussion with stakeholders and a workable alternative approach.

BSA urges CISA to recognize, explicitly, that both software producers and their customers have security responsibilities.

### B. Acknowledge that the Cause of a Cyber Incident is a Malicious Actor

The document suggests that cyber incidents are the fault of software producers. In fact, the cause of any given cyber incident is a malicious actor or actors, who are typically confident that they will not face consequences for breaking the law.

Software producers should take responsibility for those activities that are within their control, for example, following best practices for secure software development. But as the US National Cybersecurity Strategy accurately recognizes, "even the most advanced software security programs cannot prevent all vulnerabilities."

Government has the sole and exclusive responsibility of enforcing laws and conducting foreign policy. The ability of governments to deter malicious actors through meaningful consequences is a key input to a secure digital ecosystem. We applaud international efforts like the recently reported "Operation Cronos," which was both a significant achievement and important step in addressing malicious activity.

BSA recommends that CISA explicitly acknowledge both that the cause of cyber incidents are malicious actors and that they still operate in an environment in which they do not face meaningful consequences for breaking the law.

### C. Harness Market Forces

The document suggests software producers provide products or services at no additional charge.

Companies invest millions of dollars to research and develop the technologies that CISA now recognizes as valuable tools in the cybersecurity toolbelt. Technologies identified in Shifting the Balance, for example multifactor authentication, single sign-on, and secure logging, did not materialize spontaneously but are the outcome of companies' deliberate efforts. Maintaining or increasing the incentives for innovating new technologies should be a priority for CISA because that innovation is necessary to secure tomorrow's digital ecosystem.

In other contexts, policymakers have determined that customers should not have the option to purchase or conversely that producers should not have the option to sell, a product or service without a specific technology. A successful approach will not suggest that a producer not be compensated for the technologies it researches, develops, provisions, and maintains, but instead work with industry to identify consensus baseline security technologies that should be required, thereby maintaining or increasing the incentive to innovate new security technologies while improving security today.

BSA recommends industry and government collaborate to consider what technologies might be consensus baseline security technologies.

## III. Principle 2: Embrace Radical Transparency and Accountability

The document suggests software producers "embrace radical transparency and accountability" and suggests that malicious actors are finding success without transparency "providing a 'roadmap to attackers.'"

Transparency produces many benefits but also imposes costs, including demands on resources, competitive challenges, reputational risks, and legal liability. Some of the costs

associated with transparency may have supported decisions about the process followed to publish this document prior to engaging industry experts or other stakeholders. Based on this understanding, we believe that software producers should consider, understand, and account for the benefits of transparency.

We share your concern that malicious actors are finding success without roadmaps that radical transparency could provide. However, we are also concerned that providing roadmaps to malicious actors would make the current situation worse. For example, this information could make it easier for less sophisticated and less well-resourced malicious actors to find success.

BSA recommends CISA acknowledge that while transparency has benefits, it also has costs, and revisit questions like under what circumstance organizations should share information, when, with whom.

Shifting the Balance also suggests that a software producer demonstrate radical transparency by publishing information about its customers, for example what percent of customers adopted multifactor authentication or are using the latest version of a product. Transparency, while not defined, is typically understood as sharing information openly. Here, however, Shifting the Balance is not suggesting a software producer share information openly but report on its customer's activities.

BSA recommends CISA revisit how it defines transparency and consider the potential impacts of suggesting software producers report information about their customers' security activities.

One important approach to transparency identified in Shifting the Balance is the development and use of SBOMs, which BSA supports. We believe SBOMs will prove a valuable addition to cyber incident response. The document states that SBOMs will assist in purchasing decisions and operational capabilities. BSA encourages CISA to expand on its discussion and expectations on the use of SBOMs in procurement and operational activities.

Further, it appears Shifting the Balance calls for software producers to publish SBOMs before CISA's own work on SBOMs is complete. We reiterate our recommendation above that, to ensure these efforts are successful, they should proceed sequentially.

Shifting the Balance argues that transparency can help a software producer's peer organizations improve their software development practices but that software producers do not commonly publish detailed information about how they securely develop and maintain software. Notably, best practices for such activities exist, for example, BSA's Framework for Secure Software, as do other guidelines developed through public private partnerships, like the NIST SSDF, which cites the BSA Framework for Secure Software more than three dozen times. Furthermore, software producers do provide information about their security

practices in general and their secure software development practices specifically, but take a risk-based approach to publishing and sharing that information, to ensure the costs from potentially helping malicious actors is outweighed by the potential benefits to cybersecurity.

More importantly, even if CISA believes such documents and information are insufficient, it does not follow that the solution to the problem must be "radically transparent" to be effective. For example, a software producer can share information about how it creates and maintains SBOMs or share an actual SBOMs with stakeholders without making that information radically transparent and equally available to malicious actors.

BSA recommends CISA engage industry to create opportunities to share information about secure software development, and take an approach targeted to obtain the benefits of transparency without incurring unnecessary costs of transparency.

## IV. Principle 3: Lead from the Top

Shifting the Balance states, "corporate boards, including those of software manufacturers, should take a more active role in guiding cybersecurity programs," and suggests that software producers "provide regular reports to your board of directors." We agree.

Indeed, Principle 3 has the potential to be the most impactful section of the document. If a organization successfully incorporates the idea of leadership, then it will increase the likelihood that it successfully owns its security responsibilities and effectively balances the benefits and costs of transparency.

BSA recommends that the CISA expand on this principle because its successful adoption is a precursor to the other goals identified in Shifting the Balance. CISA should highlight that cybersecurity is a strategic business issue, fundamentally a risk-management practice, and ultimately influenced by leadership.

* * *

BSA appreciates the opportunity to provide the above information. We share CISA's view that "technology is integrated into nearly every facet of daily life" and believe these technologies must be continuously improved and secured. We recognize that some of the concepts and recommendations contained in Shifting the Balance must be refined but believe Shifting the Balance provides the foundation for further conversations about how software can be secured.

Henry Young
Senior Director, Policy