The Software Alliance

BSA

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

Via regulations.gov

October 31, 2023

Ms. Walden:

BSA | The Software Alliance[1] appreciates the opportunity to provide the below information in response to the Office of the National Cyber Director's (ONCD) Request for Information (RFI) on Cybersecurity Regulatory Harmonization. BSA has supported both the development of the US National Cybersecurity Strategy and the Implementation Plan and believes that collaboration 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 included harmonizing government laws and policies as a top priority in BSA's 2024 Global Cyber Agenda. Such harmonization should be based on best practices and internationally recognized standards, which supports both cybersecurity and resilience of the digital ecosystem.

[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.

BSA applauds ONCD's efforts to harmonize regulations. Resources expended on complying with multiple cybersecurity regulations increase costs to customers, including US Government agencies, without necessarily increasing security. Companies must invest heavily in identifying new and changing regulations; analyzing which regulations they must comply with and when; and making changes or documenting activities to comply with regulations, which may include reengineering products. Additionally, customers must invest in efforts to ensure that their third-party service providers are meeting any of the regulatory requirements that flow down from their regulators. The resources lost on these compliance activities cannot be invested in security improvements.

I. ONCD Should Focus on the Foundations of Regulatory Harmonization

Making meaningful progress on harmonization requires both a shared framework and binding policy guidance. Without these prerequisites, efforts to harmonize regulations are unlikely to succeed.

A. Identifying a Shared Framework

Question 3 asks about the use of existing standards and frameworks.

Without a shared framework, there is no foundation from which the US Government or any government, can drive harmonization. Even if ONCD is committed to compelling agencies to harmonize existing and new regulations, those regulations need to be harmonized to something, i.e., a framework. A framework will have the greatest odds of success if it is:

1. Developed in collaboration with industry, as all sectors of the economy will need to understand and be prepared to use the framework.
2. Based on best practices[2] and internationally recognized standards, as these will enable both improved cybersecurity management and further international harmonization.
3. Risk-based, outcome-focused, and technology-neutral, to encourage effective resource allocation, innovation, and competition.

To the extent frameworks exist that meet these criteria, for example, the NIST Cybersecurity Framework, BSA urges ONCD to leverage them.

[2] A "best practice" is, as defined by the Federal Communications Commission Communications Security, Reliability, and Interoperability Council VIII's Report on Best Practices to Improve Supply Chain Security of Infrastructure and Network Management Systems, "A method or technique that users accept as superior because it produces results that are superior to those achieved by other methods or techniques." This definition makes clear that governments cannot *create* a best practice but can *identify* and use them.

B. Publishing Binding Policy Guidance

Agencies have shown limited interest in harmonizing regulations. Without binding guidance this situation will not improve. Between the publication of the US National Cybersecurity Strategy which explicitly calls for regulatory harmonization and the present, multiple agencies have begun promulgating cybersecurity regulations that are not harmonized. Indeed, between the time ONCD published this RFI and the present, agencies have done the same.

To be successful in this important endeavor, ONCD should compel agencies to harmonize existing and new regulations. *How* ONCD does this, e.g., the creation of an office with the mission of harmonizing regulations as recommended by the President's National Security Telecommunications Advisory Committee (NSTAC), matter less than *that* agencies are required to harmonize existing and new regulations. Without this commitment efforts to harmonize regulations are unlikely to succeed.

C. Encouraging State, Local, Tribal, and Territorial Governments to Harmonize Cybersecurity Regulations.

ONCD should also encourage or incentivize state, local, tribal, and territorial (SLLT) governments to allow companies to satisfy the SLTT government's cybersecurity requirements by complying with existing cybersecurity laws or certifications. For example, if a company meets the requirements of the Federal Risk and Authorization Management Program (FedRAMP) or the Department of Defense's Cybersecurity Maturity Model Certification (CMMC) or otherwise demonstrates its cybersecurity risk management using internationally recognized standards, best practices, or certifications, then an SLTT government should consider the company to have demonstrated that it is managing cybersecurity risk and not impose further requirements.

II. ONCD Should Publish a Comprehensive Report on Cybersecurity Regulations and Pause New Regulations as it Harmonizes Existing Regulations.

Question 1 requests information on existing cybersecurity regulations.

A. Publishing a Comprehensive Report on Cybersecurity Regulations

Companies must comply with regulations issued pursuant to numerous laws. On the subject of incident reporting – for understandable reasons not the topic of this RFI, but an illustrative example nonetheless – organizations may have requirements under laws including, but not limited to, the American Recovery and Reinvestment Act, Atomic Energy Act, Bank Secrecy Act, Communications Act, Cyber Incident Reporting for Critical Infrastructure Act, Federal Information Security Modernization Act, Federal Trade Commission Act, Gramm-Leach-Bliley Act, Health Information Technology for Economic and Clinical Health Act, Protecting and Securing Chemical Facilities from Terrorist Attacks

Act, Maritime Transportation Security Act, and Sarbanes-Oxley Act. This list does not include the numerous international and state laws and similarly does not include regulations related to every cybersecurity issue other than incident reporting.

BSA appreciates the RFI seeking industry's input when exploring these cybersecurity regulations but notes that US Government agencies possess comprehensive information on their cybersecurity regulations. Importantly, US Government agencies may assert authority to promulgate cybersecurity regulations where they have not actually done so to date. In such a circumstance, a question about current regulation will fail to uncover future regulatory disharmony. An agency's assertion of authority is therefore invaluable to ONCD as it contemplates the universe of future cybersecurity regulation it must endeavor to harmonize. ONCD should obtain information about both current cybersecurity regulation and regulatory authority (e.g., from where the authority arises and under what circumstances it can be exercised) from Executive Branch agencies, and request independent agencies provide the same information or work with the Cybersecurity Forum for Independent Regulators to obtain it.

Ultimately, ONCD should publish a report that includes all this information and use it as a foundation to work with industry to determine how to prioritize the harmonization of cybersecurity regulations.

B. Pausing New Cybersecurity Regulations While Harmonizing Existing Cybersecurity Regulations

Even as the Biden-Harris Administration's US National Cybersecurity Strategy prioritizes regulatory harmonization, and ONCD undertakes this important work, US Government agencies continue to add more cybersecurity regulations which are not harmonized.

For example, the Department of Defense, General Services Administration, and National Aeronautics and Space Administration recently published a proposed rule on cyber threat and incident reporting and information sharing amending the Federal Acquisition Regulation to implement cybersecurity policies. With the understanding that the substance of cyber incident reporting is beyond the scope of this RFI, it is unclear how this proposed rule does not conflict with ONCD's efforts to harmonize cybersecurity regulations. The current situation is akin to bailing out a boat with a hole – no matter how fast one bails the water out, more water is going to come on board.

To be clear, this is not a call to end the regulation of cybersecurity but to pause new regulations as the US Government gains a wholistic understanding of the regulatory landscape; identifies a shared framework and publishes binding guidance based on that shared framework; and begins harmonizing existing and new cybersecurity regulations.

III. ONCD, through the Department of State, Should Work to Obtain Binding Commitments to Elevate Cybersecurity Over Protectionism, Harmonize Cybersecurity Regulations, and Rely on Internationally Recognized Standards.

Question 9 of the RFI seeks information about the international landscape of cybersecurity regulation.

A. Elevating Cybersecurity Over Politics and Protectionism

Many countries have or are considering laws or policies that misuse cybersecurity as a false justification for what are, in reality, protectionist trade policies. The unfortunate result of these laws and policies is to limit customers' ability to access to best-of-breed services and ultimately undermine the security of the entire digital ecosystem. ONCD and the Department of State should particularly work to avoid cybersecurity requirements that are organization-based. When a requirement applies to a product or service, a company can decide whether to develop a specific product or service for that market. This effort can be burdensome but presents a barrier to trade that a company can overcome. In contrast, organization-based requirements, e.g., local ownership, may completely preclude a company from competing in a given market, thereby depriving potential customers of more functional and secure products and services.

BSA urges ONCD to identify countries that put politics and protectionism ahead of cybersecurity. Conflating protectionism with cybersecurity will provide a false sense of security while relegating a country's organizations, including government agencies, to less functional and secure products and services.

B. Making Certifications Reciprocal: Crawling, Walking, and Running

BSA suggests ONCD and the Department of State take a crawl, walk, run approach to harmonizing cybersecurity laws and policies with international partners, as well as making them reciprocal. Countries crawl when they are aware of the security requirements of international partners and share the same language and concepts. Countries walk when they align their security requirements with those of international partners. And Countries run when they recognize the certification of international partners as sufficient assurance that a company is effectively managing cybersecurity risk.

C. Using Internationally Recognized Standards

BSA suggests ONCD and the Department of State advocate other countries adopt and enforce laws like the National Technology Transfer and Advancement Act of 1995 (NTTAA), Pub. L. 104-113, which requires US Government agencies to use international standards to carry out their policy objectives. Too often countries use national or regional standards, not to improve cybersecurity, but as non-tariff trade barriers. These efforts have multiple negative outcomes, including limiting customer's ability to select the best-of-breed solutions, and poisoning the well of cybersecurity policy by putting politics ahead of cybersecurity. If international partners adopt laws like the NTTAA, all countries, businesses, individuals, and the entire digital ecosystem would benefit.

D. Harmonizing Definitions of Critical Infrastructure

As the Biden-Harris Administration updates Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience, it should work with industry and international partners to align critical infrastructure sectors. Aligning the definitions of critical infrastructure sectors will advance intergovernmental dialogues about cybersecurity policy and reduce barriers to companies providing the most secure products and services to businesses and government agencies around the world.

IV. Moving Forward: Turning Plans into Harmonization

BSA agrees with ONCD that the lack of regulatory harmonization presents an opportunity to improve cybersecurity in multiple ways, including moving cybersecurity resources away from compliance and toward cybersecurity activities. We note that the US Government has multiple lines of effort on harmonization, as well as other areas of cybersecurity policy like open-source software security, software bills of materials, and supply chain risk management, which would similarly be improved if harmonized. We also appreciate ONCD's collaborative approach, reflected in the RFI. To achieve our shared goal of harmonized, and ultimately reciprocal, cybersecurity laws and policies, BSA suggests ONCD focus on the foundations necessary for regulatory harmonization, collecting information from US Government agencies and publish a report, as well as work internationally to bring these efforts to fruition.

We appreciate the opportunity to provide these responses and look forward to working together to achieve our shared goal.

Henry Young
Director, Policy