October 19, 2018

Ms. Linda Neilson
Director
Defense Acquisition Regulations System
United States Department of Defense

RE: Early Engagement Opportunity: Implementation of NDAA for FY 2019

Dear Director Neilson:

BSA | The Software Alliance (BSA)[1] is grateful for the opportunity to provide comments to the National Institute of Standards and Technology (NIST) on strengthening the cybersecurity of federal networks and critical infrastructure through workforce development.

BSA is the leading trade association representing the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, developing cutting-edge solutions in use across the range of information technology (IT) platforms, and are global leaders in advancing cybersecurity.

I. Introduction: BSA Input on Sections 1654 and 1655 of the FY19 NDAA

As world leaders in software development, BSA's members have a particular interest in the implementation of Sections 1654 and 1655 of the Fiscal Year 2019 National Defense Authorization Act (H.R. 5515; Public Law 115-232) (FY19 NDAA), which direct the establishment of a Department of Defense program intended to mitigate risks derivative of foreign governments' code review of information technology products used by the Department. In the *Joint Explanatory Statement* (JES) accompanying the bill, conferees emphasize the need to balance the policy's aim to "minimize[e] the supply chain risk posed by companies like Kaspersky" with "actions to minimize the potential injury of the non-use requirement, to both the Department and industry." BSA is grateful for the opportunity to provide input to the Department as it seeks to draft implementing regulations that capture this balance.

BSA acknowledges the real and growing cybersecurity risks to the Department's supply chain, and strongly support efforts to improve the Department's ability to identify, prevent, and mitigate these risks. BSA also strongly supports the Department's drive toward improving its innovation and technological agility. Our input aims to ensure that implementation of Sections 1654 and 1655 mutually supports both of these objectives.

---

[1] BSA's members include: Adobe, Akamai, ANSYS, Apple, Autodesk, Bentley Systems, Box, CA Technologies, Cadence, CNC/Mastercam, DataStax, Docusign, IBM, Informatica, Microsoft, Okta, Oracle, PTC, salesforce.com, SAS Institute, Siemens PLM Software, Slack, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro, and Workday.

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org

To that end, as the Department considers regulations implementing Sections 1654 and 1655, we propose that five areas represent key building blocks for a policy that successfully balances the Department's objectives with regard to supply chains security and technological innovation: (1) providing detailed input on identifying countries of particular concern; (2) defining the scope of code reviews; (3) establishing criteria for *de minimus* reviews; (4) protecting business confidentiality; and (5) developing a third-party testing standard. Each of these building blocks is examined in further detail below.

II. Countries of Particular Concern.

Section 1654 directs the Secretary of Defense to create a list of countries that "pose a risk to the cybersecurity of United States defense and national security systems and infrastructure." While Congress directs the Secretary to consider a broad range of criteria (including some – like force protection risks or engagement in foreign intelligence activities – that are not specific to cybersecurity), the list is ultimately intended to serve as a tool to scope the non-use and disclosure requirements outlined by Section 1655. As such, the list should be narrowly targeted to cover only those countries who, through the process of government-mandated or -conducted reviews of source code of products used by the Department of Defense, pose a risk to the cybersecurity of US defense and national security systems and infrastructure.

Specifically, the Secretary should consider the following:

1) Whether a country conducts, or has established policies that require, source code reviews;
2) Whether a country conducts, or has an established record of conducting, cyber activities and operations to affect the cyber defenses or supply chain of the United States Government;
3) Whether a country conducts, or has an established record of conducting, cyber activities to gain unauthorized access to the intellectual property of US businesses or persons; and
4) Whether a country has sufficient technical capacity to conceivably use cyber means to exploit a source code review process to interfere with, gain unauthorized access to, or gain inappropriate knowledge of a product submitted for such a review.

By narrowly scoping the Countries of Particular Concern list, the Department will ensure that the non-use and disclosure requirements of Section 1655 are appropriately calibrated to address high-risk scenarios without creating overly burdensome compliance requirements for US businesses or unnecessarily impacting US diplomatic relations.

III. Defining the scope of code reviews.

Section 1655 prohibits the Department of Defense from using certain types technology, including information and operational technology and cybersecurity services, unless the provider of the technology notifies the Department when it has permitted certain foreign actors to review the code of such the product, system, or service being provided to the Department. <u>It is essential that the implementing regulations carefully define the scope of technologies to which this requirement applies and the scope of circumstances in which it applies.</u> Specifically, the regulation should address:

- *What products, systems, and services are covered.* The regulation should define the scope of products, systems, and services covered by the non-use requirement according to the varying levels of risk such technologies may pose

to the Department. For example, the risk associated with a foreign actor's access to code relating to highly sensitive, customized software supporting major weapons systems must be calculated far differently than the risk associated with commonly used workplace productivity software. In passing the final version of the FY19 NDAA, conferees argued in their JES that the Secretary of Defense should "exempt from this requirement any product, system, or service if: (1) Its source code has been exported pursuant to a license or license exception granted under the Export Administration Regulations (15 C.F.R. §§ 730774); (2) It is not itself, and is not a component of, a National Security System; (3) It is not a cybersecurity tool, system, or application or does not have a built-in cybersecurity tool, system, or application; or (4) It is subjected only to a de minimis disclosure under restricted access conditions, as defined by the Secretary." These proposed exemptions make good sense, and should be included in the implementing regulations. Proposed exemptions (2) and (3) would ensure that the non-use requirements target the most high-risk software, rather than widely used commercial off-the-shelf software, office productivity software, and other products where risk is limited or not unique to the Department. Finally, the legislation exempts open source software from its non-use requirements; implementing regulations should clarify that open source software is exempted even if it is included as a component of otherwise covered products, systems, or services.

- *What a code review is.* As the conferees noted in the Joint Explanatory Statement, the program is intended to "mitigate the risks derivative of foreign governments' code review of information technology products used by the Department of Defense." While the legislation does not define "code review," it is clear that it intended the non-use and disclosure requirements to apply to a specific type of activity in which foreign governments formally direct a process involving the review of portions of the code of a product, service, or system, or the submission of portions of that code to code-scanning and related tools. The regulations should carefully delineate the circumstances that constitute a code review in order to avoid confusion about either processes or foreign actors that could trigger these requirements.

  The Department should consider the following definition of source code review:

  > "***Code review:*** A process wherein, in response to the direction of a foreign government, an agency of a foreign government, or an official acting on behalf of a foreign government, a vendor formally submits portions of the software code of a product, service, or system to a third party for a quality assurance review using human and/or automated methodologies. A code review is normally conducted in a laboratory or other controlled setting, and may involve the use of automated static analysis or other anomaly detection tools."

- *What foreign actors are covered.* Section 1655 discusses requirements deriving from instances in which a vendor subjects, or is obligated to subject, its code to a "foreign government or foreign person" for code review. Implementing regulations should clarify that these requirements apply only to code reviews involving foreign persons who are acting in an official capacity on behalf of, at the official direction of, or through a direct contractual relationship with a foreign government. This clarification would distinguish between, for example, an independent testing laboratory conducting a code review on behalf of a foreign

government and a non-government-affiliated foreign person conducting code review for quality assurance during software development on behalf of a vendor or for an accredited certification process.

- *To what extent requirements extend to contractual partners or suppliers.* Many software developers integrate third-party components into their software products or enter into business partnerships with third-party partners. Even when establishing measures to ensure supply chain transparency and security, a vendor may not be able to prevent a supplier or contractual partner from subjecting portions of a codebase to a code review meeting the criteria set forth by Section 1655 without the vendor's knowledge. Implementing regulations should oblige vendors to disclose when a third party has subjected portions of the relevant codebase to a code review only in instances when the vendor has knowledge of the code review, provided that the vendor takes reasonable measures to maintain awareness of such activities by its third-party suppliers or contractual partners.

IV. Establishing criteria for "de minimus" reviews.

In the Joint Explanatory Statement accompanying the legislation, conferees encouraged the Secretary to provide for products, services, and systems to be exempted from non-use and disclosure requirements set forth in Section 1655 if they are "subjected only to a de minimis disclosure under restricted access conditions, as defined by the Secretary." Establishing reasonable criteria for a *de minimus* review would allow the Department to focus its scrutiny on the most high-risk code review activities, minimizing unnecessary processes and compliance requirements in instances where compromise of a product, service, or system is highly unlikely.

For the purposes of applying exemptions to non-use and disclosure requirements set forth in Section 1655, the implementing regulations should define *de minimus* disclosures as those code reviews that meet the following criteria:

1) The code review involves disclosure of less than two percent of the source code of the subject product, system, or service;
2) The code subject to the code review is identified by an automated scanning tool from an internationally recognized provider of such tools;
3) The code review and related analysis are conducted at a vendor-controlled facility or at an internationally accredited independent laboratory facility located outside a country identified in the Countries of Particular Concern list created under Section 1654;
4) Automated code scanning and analysis conducted in relation to the code review are conducted by the vendor or by an independent and internationally recognized third party in the presence of the vendor;
5) The code review involves no recording devices;
6) Parties receive a paper summary of results, and no other materials associated with the code review are provided or permitted to leave the facility; and
7) The code review complies with any relevant internationally recognized standards.

V. Protecting business confidentiality.

Disclosures required under the legislation could require vendors to provide information that is confidential business information and could, if made public, expose sensitive business strategies, proprietary product information, or other information that could potentially damage vendors. To prevent such harm, the implementing regulations should explicitly exempt any information shared as part of a required disclosure from federal, state, and local freedom of information laws, open government laws, open meetings laws, open records laws, sunshine laws, and similar laws requiring disclosure of information or records.

Further, the regulations should make clear that information disclosed by vendors should be used strictly to improve the Department's risk management posture. They should make clear that the information disclosed to the government cannot be used to inform any contract actions such as the award, modification, or termination of a government contract, or for any civil or criminal action against the disclosing company. Implementing regulations should limit requesting agencies' access to the registry established under Section 1655(f) to federal authorities (e.g., procurement officials) who have a need to know. Access to the registry should be tracked, audited, and enforced.

Finally, Section 1655 requires an annual report to Congress on disclosures made under the non-use requirements. Similar precautions should be taken to ensure that sensitive information is not made public; specifically, in addition to confidential business information, the Department should avoid mentioning company names, specific products, or other publicly identifiable information in these reports.

VI. Establishing a third-party testing standard.

Section 1655(d)(2) requires the Secretary to "develop such third-party testing standard as the Secretary considers acceptable for commercial off the shelf (COTS) products, systems, or services to use when dealing with foreign governments." While Congress's interest in such a standard is understandable, it presents a risk: development of a standard focusing on foreign government code reviews would potentially normalize the practice of such reviews, which could increase the prevalence of government policies mandating such reviews.

The Department should focus its efforts on developing a standard for accrediting independent laboratories that conduct code reviews, including those that are directed by foreign governments. Vendors may have a variety of reasons for subjecting products to code reviews at independent laboratories, including to support internal quality assurance efforts. Focusing on accrediting independent laboratories could help to build a more trusted infrastructure for vendors to work through in satisfying foreign government requirements without suggesting that such requirements are appropriate or acceptable.

In developing this standard, the Department should begin by considering ISO/IEC 17025:2017, which specifies "general requirements for the competence, impartiality and consistent operation of laboratories." The Department could also consider establishing compliance with the criteria set for *de minimus* code reviews as a requirement for accreditation.

VII. Conclusion

Enhancing the security of the Department of Defense's supply chain and software base will require effective collaboration between the Department and the software industry. By

crafting implementing regulations in support of Sections 1654 and 1655 according to the building blocks outlines above, the Department can lay the foundation for such collaboration without creating undue burdens on industry stakeholders or stifling innovation. BSA and its members are eager to work with the Department as these implementing regulations are drafted, finalized, and implemented. We look forward to more detailed discussions as these policies evolve.

Thank you for the opportunity to comment on this important matter.

Sincerely,

Tommy Ross
Senior Director, Policy