



November 9, 2020

Matthew S. Borman  
Deputy Assistant Secretary for Export Administration  
Bureau of Industry and Security  
U.S. Department of Commerce  
Room 2099B  
14<sup>th</sup> Street and Pennsylvania Avenue NW  
Washington, DC 20230

**RE: Advance Notice of Proposed Rulemaking on Foundational Technologies [RIN 0694-AH80]**

Dear Mr. Borman,

BSA | The Software Alliance appreciates this opportunity to provide comments to the Bureau of Industry and Security (“BIS”) in response to the Advance Notice of Proposed Rulemaking (“ANPRM”) regarding the “Identification and Review of Controls for Certain Foundational Technologies.”<sup>1</sup> BSA is the leading advocate for the global software industry before governments and in the international marketplace.<sup>2</sup> The software industry contributes more than \$1.6 trillion to U.S. GDP and supports 14.4 million U.S. jobs.<sup>3</sup> Software, combined with the more than \$82.7 billion that the industry invests annually in research and development, serves as a powerful catalyst for U.S. economic growth, making companies more competitive and the economy more robust.

---

<sup>1</sup> 85 Fed. Reg. 167, 52934 (Dep’t Commerce Aug. 27, 2020).

<sup>2</sup> BSA’s members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

<sup>3</sup> See Software.org: The BSA Foundation, *Software: Growing US Jobs and the GDP* (2019), available at <https://software.org/wp-content/uploads/2019SoftwareJobs.pdf>.

BSA understands and shares the legitimate concerns expressed by Congress in the Export Control Reform Act of 2018 (“ECRA”)<sup>4</sup> and supports the effort to modernize the Export Administration Regulations’ (“EAR”) coverage of “emerging” and “foundational technologies” that are essential to US national security. Of course, as both ECRA and the ANPRM acknowledge, the Administration’s national security objectives can be achieved only through a careful balancing of equities, including the strategic imperative of ensuring that the United States remains the global hub for innovation. Achieving this balance and preserving the United States’ competitive advantage in the development of new technologies that are critical to economic growth and security therefore requires a “small yard, high fence” approach to export controls that is focused on narrowly defining the technologies that are essential to long-term national security and aggressively defending them.<sup>5</sup> Consistent with this approach, we offer below a series of recommendations that BIS should consider as it defines the foundational technologies that may become subject to heightened control under the EAR.

### **Criteria for Identifying Foundational Technologies**

As both ECRA and the ANPRM acknowledge, the “national security of the United States requires that the United States maintain its leadership in the science, technology, engineering, and manufacturing sectors, including foundational technology that is essential to innovation.”<sup>6</sup> Recognizing that overly-broad export controls would undermine such leadership, ECRA includes a number of important safeguards that should serve as criteria for defining “foundational technologies” and identifying the particular items that may warrant more restrictive control.

- ***Foundational Technologies Must Not be Widely Available From Foreign Suppliers***

In reforming ECRA, Congress recognized the application of unilateral export controls on “items widely available from foreign sources” are generally ineffective.<sup>7</sup> Therefore, prior to deeming a technology “foundational,” ECRA requires BIS to determine whether it is also under development in foreign countries and whether

---

<sup>4</sup> Enacted as part of the National Defense Authorization Act for Fiscal Year 2019, Public Law No: 115-232.

<sup>5</sup> Lorand Laskai and Samm Sacks, *The Right Way to Defend America’s Innovation Strategy*, Foreign Policy (Oct. 28, 2018), available at <https://www.foreignaffairs.com/articles/2018-10-23/right-way-protect-americas-innovation-advantage>.

<sup>6</sup> ECRA § 1752(3).

<sup>7</sup> ECRA § 1752(6).

an export control could effectively limit its international “proliferation.”<sup>8</sup> Simply put, a unilateral control cannot limit the proliferation of a technology that is widely available from foreign suppliers. Subjecting such technologies to control will disadvantage US companies without advancing any corresponding national security interest. Countries of concern targeted by unilateral controls that can no longer rely on US tech will advance their own indigenous solutions, competing with US tech on the global market. Multinational companies – located outside of countries targeted by these controls – will turn to these alternatives in lieu of having to use different tech for different regions. US companies will lose out on the world’s best scientists and engineers, who will look for work in less restrictive regulatory environments. Thus, a critical criterion for identifying an “foundational technology” is its foreign availability: technologies that are widely available from foreign suppliers should not be considered foundational.

- ***Foundational Technologies Must Be Narrowly Tailored and Well-Defined***

Congress has directed that national security-related export controls must be carefully “tailored to focus on...core technologies” that pose a security threat to the United States,<sup>9</sup> and that they must likewise be “transparent, predictable, and timely.”<sup>10</sup> Congress imposed such requirements to ensure export controls are narrowly tailored to achieve their intended national security objectives and so that there is certainty about the specific technologies that are subject to control. To satisfy this requirement, BIS should commit to identifying “foundational technologies” using the existing Export Control Classification Number (“ECCN”) system in its Commerce Control List and clear, carefully scoped definitions. Furthermore, BIS should rely on “end-user” and “end-use” controls to target uses and users of concern while allowing exports for beneficial purposes and to trustworthy parties to continue. In all cases, it is critical to maintain explicit exemptions from any controls on technologies that are widely available from foreign suppliers. There are opportunities to digitally transform the export control system through increased reliance on end-use and end-user controls that are backed by software- and/or hardware-based tools to facilitate continuous monitoring and enforcement against unauthorized uses and users. Such solutions are already used in familiar settings such as app stores, in which operators use technology-based permissions to determine whether apps fulfill policies on privacy, security, and other requirements; and the encryption modules in secure payment systems. Such a digital transformation of export controls could make them more

---

<sup>8</sup> ECRA § 1758(a)(2)(B).

<sup>9</sup> ECRA § 1752(2)(G).

<sup>10</sup> ECRA § 1752(8).

effective, more dynamic, and more comprehensive while preserving US technological leadership.

- ***Foundational Technologies Must be Essential to Specific US National Security Interests***

ECRA likewise directs BIS to narrowly focus on “foundational technologies” that are “essential to the national security of the United States.”<sup>11</sup> Although the EAR does not define “essential,” technology controls in the EAR are limited to aspects of technology that are “required,” or “peculiarly responsible,” for achieving a controlled characteristic, function, or capability. Accordingly, technologies should be considered “essential” with reference to a military capability only if required, or peculiarly responsible for achieving the relevant (and specific) military capability.

- ***Foundational Technology Controls Must be Consistent with the Core Values that have Driven US Innovation***

Technology controls are ultimately a tool for preventing adversaries from gaining access to innovations that could be used to undermine US national security. At the same time, Congress and the Administration have acknowledged that long-term national security is reliant on the US remaining the global leader in the development of emerging technologies.<sup>12</sup> As such, technology controls should be carefully calibrated to avoid harming the R&D capacity, engineering skill, commercial competitiveness, and other key features that have made America the global hub for innovation. It is imperative, for instance, to ensure that controls will not impair the ability of US companies and academic institutions to collaborate with foreign colleagues on fundamental research efforts, standards development processes, or other open source projects that rely on international collaboration. Foundational technology controls should likewise account for the benefits that US companies derive from recruiting and employing the best talent from around the world. To avoid impacting such projects that are in-progress and for which significant investments may already have been made, any new controls should exclude requirements for deemed export licenses, particularly for foundational technologies that have been previously released to authorized foreign nationals.

---

<sup>11</sup> ECRA § 1758(a)(1)(A) (emphasis added).

<sup>12</sup> ECRA Sec. 1752(3); See *also*, Remarks by U.S. Commerce Secretary Wilbur L. Ross at the Bureau of Industry and Security Annual Conference on Export Controls and Security (July 9, 2019), <https://www.commerce.gov/news/speeches/2019/07/remarks-us-commerce-secretary-wilbur-l-ross-bureau-industry-and-security>.

- **Software Cannot be a “Foundational Technology”**

By focusing narrowly on “technologies” that are “foundational,” Congress sought to limit the scope of any potential export controls. The reference to “technology” must be understood as limiting the reach of any resulting export controls to specific forms of *information* necessary for the development of sensitive products or services, as opposed to controls on commodities or software. Indeed, Section 1742 of ECRA defines “technology,” consistent with the definition in the EAR,<sup>13</sup> to include “information, in tangible or intangible form, necessary for the development, production, or use of an item.” By comparison, Section 1742(7) defines “item” as a “commodity, software, or technology.” Thus, the final rule must be limited to possible new controls on information that is within the scope of the term “technology,” and does not include possible new controls on “software” or any other “item.”

### **Application of Criteria to Military End-Use/End-User Items**

The ANPRM signals that BIS is evaluating whether “items that are subject to control for military end use or military end user reasons” under EAR Section 744.21 (MEU Rule) should be deemed foundational technologies. Consistent with the abovementioned criteria, we urge BIS to take a cautious and methodical approach in determining whether particular items subject to the MEU Rule should also be deemed “foundational. While some items that are subject to the MEU Rule may meet the criteria outlined above, many do not.

Recent changes to the MEU Rule expand its reach to a wide swath of commonplace technologies that are widely available from foreign suppliers and far removed from any “essential” national security interest.<sup>14</sup> For instance, the expanded MEU Rule now includes “mass-market encryption items” controlled under ECCN 5A992 and 5D992 on the EAR’s Commerce Control List (“CCL”). These broad categories include common enterprise productivity software that BSA members sell around the world and software widely installed on individual or business computers and devices. These products are neither sensitive nor unique to the US market, and already are available worldwide, including in China, Russia, and Venezuela. Because the covered items are ubiquitous, imposing restrictions on just the subset of such items subject to US export controls jurisdiction places producers of those items at a competitive disadvantage, without any clear impact

---

<sup>13</sup> See EAR § 772.1 (definition of technology).

<sup>14</sup> See *Expansion of Export, Reexport, and Transfer (in-Country) Controls for Military End Use or Military End Users in the People’s Republic of China, Russia, or Venezuela*, 85 Fed. Reg. 23,459 (Apr. 28, 2020).

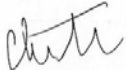
on the military capabilities of the relevant countries. This competitive disadvantage affects U.S. producers globally, to the extent that multinational customers do not want to rely on tech they can use in, for example, Europe, but not in China or Russia.

We are troubled by BIS's decision to expand the MEU Rule to include mass market encryption items. These concerns would be exacerbated if mass market encryption items were now to be deemed "foundational technologies" merely by virtue of their inclusion in the expanded MEU Rule. Instead, BIS should commit to analyzing individual ECCNs (including those that are subject to the MEU Rule) against the criteria set forth in ECRA (and noted above) to determine whether they can appropriately be deemed "foundational technologies." Given BIS's conclusion in 2007 that mass-market encryption items are widely available from foreign suppliers and that subjecting them to US control "would not make an impact on the military capability" of US adversaries,<sup>15</sup> BSA respectfully submits that it would be inappropriate to deem such items as "foundational technologies" or to subject them to heightened controls.

\* \* \* \*

BSA appreciates the opportunity to provide initial input regarding appropriate criteria for defining "foundational technology" and look forward to remaining engaged with BIS and the broader interagency as this process moves forward. Of course, defining the term "foundational technology" is merely the first step in a longer process that will involve identifying the specific items that should be subject to control under the EAR. To ensure that BIS receives all of the information it needs to balance the equities that are at stake when it comes to the application of new export controls (e.g., performing a foreign availability analysis), it is imperative that industry is afforded the opportunity provide feedback on specific items that BIS proposes to classify as "foundational technologies." Accordingly, we urge BIS to commit to issuing additional Notices of Proposed Rule Making that identify the specific ECCN control parameters, license requirements and license exception eligibilities that would apply to any newly proposed controls.

Sincerely,



Christian Troncoso  
Senior Director, Policy

---

<sup>15</sup> See *Revisions and Clarification of Export and Reexport Controls for the People's Republic of China (PRC); New Authorization Validated End-User; Revision of Import Certificate and PRC End-User Statement Requirements*, 72 Fed. Reg. 33,646, 33,648 (June 19, 2007).