



November 9, 2020

Comments submitted via the Federal eRulemaking Portal: <http://www.regulations.gov>

Tongele Tongele
Office of Nonproliferation and Treaty Compliance
Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, D.C. 20230

Subject: Identification and Review of Controls for Certain Foundational Technologies

Reference: RIN 0694-AH80– Federal Register / Vol. 85, No. 167 / Thursday, August 27, 2020 /
Advanced Notice of Proposed Rulemaking (ANPRM)

Dear Dr. Tongele:

The Computing Technology Industry Association (CompTIA), the leading association for the global information technology (IT) industry, thanks you for your time in reviewing our responses to the ANPRM for the identification and review of controls for certain foundational technologies. We fully recognize the importance of the technology industry partnering with BIS on the identification of technologies critical to national security. In general, we urge BIS to continue seeking industry feedback through proposed rules and provide for transition periods with adequate time for industry to implement internal processes to meet the additional regulatory burden.

General Comments on Foundational Technology Controls

At the outset, we urge caution in imposing new and/or additional licensing requirements on items that have previously been determined by the U.S. Department of Commerce as part of its standard rulemaking process to warrant no control or only anti-terrorism (AT) level controls. Such determinations, which were the product of careful and thorough interagency analysis, have become deeply ingrained into technology companies' export compliance policies and programs around the world. As such, the "foundational technology" concept should not be a basis for wholesale reappraisal of longstanding regulatory assessments.

Instead, we view the statutory requirements to identify “foundational technologies” as inextricably linked to the requirement to identify “emerging technologies.” Indeed, the relevant statutory language calls the establishment of a “regular, ongoing interagency process to identify emerging and foundational technologies.”¹ Notably, the statute does not contemplate two independent processes for identifying emerging technologies and foundational technologies, respectively. The implication is that emerging and foundational technologies should be identified together. This reading of the statute is consistent with what we believe to be the most significant national security concerns around mature technologies, namely that technologies previously determined to not warrant heightened licensing requirements based on the known uses at the time of the assessment may find new purposes as critical enablers of emerging technologies.

Rather than trying to identify foundational technologies in a vacuum, the Commerce Department and other relevant agencies should first focus on identifying emerging technologies warranting heightened multilateral controls based on national security concerns. Once these emerging technologies are identified multilaterally², the Commerce Department and its counterparts (with assistance from the advisory committees and other input from industry and academia) should identify existing, fully-mature technologies that, because of novel uses, are critical to (i.e., required for) the development, production, or use of controlled emerging technologies.

Only such fully mature technologies with novel uses critical to these emerging technologies should warrant consideration for control as foundational technologies. Moreover, these foundational technology controls should be narrowly scoped to the uses of any identified technology that is relevant to an emerging technology. For instance, foundational technology controls should not be applied to the entire corpus of technical data generated for technologies over the decades that it has existed. Instead, foundational technology controls should be limited to the implementations of these technologies that relate to the identified emerging technology.

Responses to Specific Questions:

Based on the conceptual approach outlined above, we have addressed each of the questions posed by the ANPRM in an effort to provide clarity and be responsive to the notice.

¹ 50 USC 4817(a)(i) (emphasis added).

² We note that 50 U.S.C. § 4817(c)(2) states that if a unilateral control is not adopted by a multilateral regime within a 3-year period, the control should be removed.

1. How to further define foundational technology to assist in identification of such items

We propose that BIS define the following as “foundational technologies” in Part 772 of the Export Administration Regulations (EAR), noting that much of the language used is already found in several parts in the EAR:

Technologies that are:

- i. Subject to the EAR*
- ii. Fully mature, not developmental or pre-commercial (i.e., not emerging technologies);*
- iii. Essential to national security, meaning that the technology is peculiarly responsible for achieving or exceeding performance levels, characteristics or functions that provide a significant contribution (i.e., specific, identifiable, qualitative advantage) to the military potential of the United States or any other country or combination of countries in terms of conventional weapons, intelligence collection, weapons of mass destruction, or terrorist or anti-terrorist capabilities, as determined by the U.S. government, and stated in the EAR;*
- iv. “Specially designed” for the “development,” “production,” or “use” of an emerging technology described on the Commerce Control List;*
- v. Not already designed or manufactured or being developed;*
 - a. Outside of the United States (in the case of a control imposed unilaterally), or*
 - b. Outside of the United States and closely allied nations (in the case of a control adopted by a multilateral export control regime, such as the Wassenaar Arrangement).*

While we believe this definition captures the criteria that would help in identifying foundational technologies worthy of BIS review, we note that the pool of technologies that would qualify would likely be very small. As such, and as described further below, we believe the best approach would be to focus efforts on identifying emerging technologies that are more likely to pose a national security concern and requesting industry input for any implications for foundational technologies that meet the criteria above and could reasonably be considered. Lastly, we believe that BIS should limit its scope to technologies and refrain from including commodities and software in the controls.

2. Sources to identify such items

Based on this definition, we believe the best approach to identifying foundational technologies would be to begin with the efforts to identify emerging technologies warranting control under the

EAR. The process for identifying such emerging technologies was the subject of the 2018 ANPRM and is outside of the scope of this request.

Once an emerging technology warranting controls has been identified, BIS should seek public input to identify the existing technologies that are critical for the development, production and use of the newly controlled emerging technology. This set of existing technologies should then be subjected to analysis under the remaining requirements in the test outlined above: namely, whether the emerging technology is relying on a specially designed implementation of the existing technology, whether this specially designed implementation has foreign availability, and whether it is possible to develop controls that are narrowly tailored to the specially designed implementation.

3. Criteria to determine whether controlled items identified in AT level Export Control Classification Numbers (ECCNs), in whole or in part, or covered by EAR99 categories, for which a license is not required to countries subject to a U.S. arms embargo, are essential to U.S. national security

As was noted above, we urge caution in imposing new controls on items previously controlled for AT reasons or classified as EAR99. However, we believe that the test set out above will balance regulatory stability with the changing technical landscape since it will limit potential controls to technologies that are tailored to specially designed implementations in emerging technologies.

By way of example, if an existing EAR99-controlled technology is being used in a common, non-specialized implementation to support the development, production or use of an emerging technology, the proposed test would not support reclassification of the entire technology as subject to heightened controls. Application of heightened controls should only occur if (among other things) there is some narrow implementation of that existing EAR99 mature technology that is specially designed for the development, production, or use of an emerging technology. All other implementations of the existing technology would remain EAR99.

4. The status of development of foundational technologies in the United States and other countries

Mass-market encryption items classified under ECCNs 5A992 and 5D992 are a useful example of how deregulation positively contributes to U.S. development and influence in the technology sector. Mass-market status is premised in part on the ubiquity of the technology – i.e., one criterion to qualify for a 5A992 or 5D992 classification is that the item in question must be “generally available to the public[.]” BIS simplified the mass market classification in 2010 by

allowing immediate authorization for the export of “Less Sensitive Encryption Items and Certain Mass Market Encryption Items.”

These changes were made to correct overly broad encryption controls and “enhance national security by ensuring the continued competitiveness of U.S. encryption products.”³ This rationale continues to apply and 5A992 or 5D992 items that were relatively recently decontrolled to enhance national security should not now be subject to new, ineffective controls. As BIS notes in its rationale, such controls have the potential to diminish U.S. national security by reducing the competitiveness of U.S. encryption products. Additionally, 5A992 and 5D992 items are already subject to the recently expanded military end-use/user controls in Supplement 2 to Section 744.21 of the EAR.⁴

To elaborate further, much of the hardware and software that provides the basic technological infrastructure for business and entertainment in offices, data centers, and homes around the world (e.g., servers, laptops, word-processing software, smart speakers, smart TVs) is classified under these “mass-market” encryption categories. Imposing additional “foundational” restrictions on these items, even in a limited number of countries like China or Russia, would effectively cut off U.S. consumer and enterprise electronics companies from access to these massive markets as well as other markets globally where multinational companies prefer not to rely on technology they can use in, for example, Europe, but not in China or Russia. That gap will then be filled by foreign companies, potentially even by the very countries the controls target, which will harm U.S. industry and U.S. national security by diminishing the overall use and influence of American products and companies abroad, and by providing an economic and diplomatic boost to companies like Huawei who are well positioned to saturate these markets with less secure technology. This may also create a schism in global encryption standards wherein more products will begin using proprietary encryption standards developed by foreign governments rather than globally accepted standards, such as AES-128.

Microprocessor Hardware and Technology

Design of Commerce Control List Category 3 semiconductor technology takes place all over the world, including the U.S., Taiwan, the United Kingdom, South Korea, and Israel (where U.S. companies have substantial design centers), and U.S. semiconductor companies also work with design teams throughout the world. Additionally, global companies, including at least one

³ See, e.g., Encryption Export Controls: Revision of License Exception ENC and Mass Market Eligibility, 75 Fed. Reg. 36481, at 36483 (June 25, 2010), available at <https://www.federalregister.gov/documents/2010/06/25/2010-15072/encryption-export-controls-revision-of-license-exception-enc-and-mass-market-eligibility-submission>.

⁴ The ANPRM specifically identifies technologies identified in this supplement as potential candidates for regulation (“foundational technologies could include items that are currently subject to control for military end use or military end user reasons under Supplement No. 2 to part 744 of the EAR”).

Chinese company, Alibaba, are already using the RISC-V “free and open” instruction set architecture to develop high-performing microprocessors based on information that is “published” and therefore not subject to the EAR.⁵ In light of these design and development activities, additional controls on exports of microprocessors and microprocessor design technology would be ineffective in achieving the government’s national security goals because microprocessor design activity is already dispersed and available globally. However, limiting the ability of U.S. companies to export microprocessors and microprocessor designs would provide a competitive advantage to non-U.S. companies in this industry.

BIS has already taken steps through the expansion of the foreign direct product rule, Entity List (Huawei, HiSilicon), and licensing requirements and policies applied to SMIC and other Chinese companies of concern, in order to cut off these companies’ access to certain EAR99 and AT-level U.S. technologies that might be deemed to be “foundational.” As demonstrated by these examples, targeted measures, such as Entity List designations are much more effective mechanisms for limiting technological development in countries of concern as opposed to, e.g., limiting the export of commercial 3A991 or 3A992 hardware that is already widely available around the world. As a result, it is highly unlikely that unilateral export controls on 3A991 or 3A992 hardware or 3E991 technology would result in national security gains that have not already been accomplished by other recent controls. At a minimum, BIS should carefully analyze the impact of the new end-use/end-user based restrictions recently imposed on Russia, Venezuela, China, and various Chinese companies before imposing any new list-based restrictions on “foundational technologies” to serve the same purpose as these existing restrictions.

5. The impact specific foundational technology controls may have on the development of such technologies in the U.S.

Regarding the impact specific foundational technology controls may have on the development of such technologies in the U.S., it is essential that BIS refrain from imposing controls on items having substantial foreign availability. For example, no XX99X ECCNs are controlled at the multilateral level, and thus placing unilateral controls on these items would disadvantage companies in the United States and could cause companies outside the U.S. to exclude U.S. technologies and components from their designs. This would have a significant negative impact on the U.S. economy and undermine U.S. technological leadership. Countries of concern targeted by unilateral controls will advance their own indigenous solutions, and seek technology partnerships with non-U.S. companies, competing with U.S. technology and diminishing global market share of U.S. companies. Multinational companies – located outside of countries targeted

⁵ <https://riscv.org/about/>

by these controls – will turn to these alternatives in lieu of having to use different technology for different regions.

At the same time, creating new deemed export licensing requirements would hamper (if not deter) some of the world’s best scientists and engineers from contributing to U.S. technical efforts. This would undermine a core mission of ECRA: allowing the U.S. to “...maintain its leadership in the science, technology, engineering, and manufacturing sectors, including foundational technology that is essential to innovation.”⁶ Additionally, the ability of technology companies, including semiconductor companies, to continue funding cutting-edge research and innovation in the United States depends on their ability to access global markets and sell products and related technologies around the world.

6. Examples of implementing controls based on end-use and/or end-user rather than, or in addition to, technology-based controls

Before proceeding with any end-use or end-user controls related to foundational technologies, we would encourage BIS to develop regulations that lend themselves to workable and scalable compliance implementations. Regulations that cannot be easily implemented by industry do not serve to achieve BIS’ policy objectives. To the extent that BIS determines that end-user considerations are essential for achieving national security interests, we strongly believe that any such end-user controls be explicit, and focused on identified end users, e.g., entries on the Entity List. Most companies that trade in controlled items products have sophisticated screening systems to monitor customer bases against changes to the BIS Entity List or OFAC’s SDN list. At the same time, opaque ownership structures and the complexity of systematically determining what activity is authorized can pose challenges for screening approaches. End-use restrictions, when specific, may be useful for addressing nefarious uses of greatest concern but can be difficult to detect at scale. In light of these limitations, we suggest that Commerce explore the potential for use of novel technological solutions to implement end-use and end-user controls more nimbly on the most sensitive technologies. Such a digital transformation of export controls could make them more effective, more dynamic, and more comprehensive while preserving U.S. technological leadership.

7. Any enabling technologies, including tooling, testing, and certification equipment, that should be included within the scope of a foundational technology

Any new controls on testing and certification equipment carry the potentially catastrophic, additional risk that international testing and certification regimes will shift to less-controlled (and potentially Chinese-dominated) systems of industry standards.

⁶ 50 U.S.C. § 4811(3).

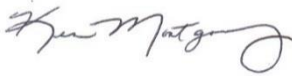
8. Any other approaches to the issue of identifying foundational technologies important to U.S. national security, including the stage of development or maturity level of a foundational technology that would warrant consideration for export control.

We believe list-based controls are more readily tailored to address national security concerns without imposing harmful collateral consequences at issue for benign commercial applications, regardless of the maturity or development level of a foundational technology.

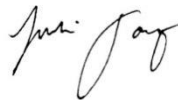
We appreciate your time in reviewing our concerns and recommendations. The potential impact of specific foundational technologies controls demonstrates that new licensing requirements BIS considers should be limited to the specific implementation of an existing technology which poses national security concerns because it is critical for an identified emerging technology subject to heightened control, rather than an entirely mature, well-established technical domain.

We believe limiting foundational technology controls to a narrow set of criteria and implementation for critical emerging technologies will better meet the policy rationale of ECRA and ensure consistency within the EAR, especially given that relevant language already exists in the EAR for a potential definition. We look forward to continuing engagement on this matter.

Sincerely,



Ken Montgomery
Vice President
International Trade Regulation & Compliance



Juhi Tariq
Senior Manager
International Trade Regulation & Compliance