January 10, 2019

Via eRulemaking Portal (http://www.regulations.gov): BIS 2018-0024

Ms. Hillary Hess
Director, Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
Washington, DC 20230

REF: RIN 0694–AH61

RE: Comments on Proposed Criteria for Identifying Emerging Technologies

Dear Ms. Hess:

The American Bar Association (“ABA”) Section of International Law (“Section”) appreciates the opportunity to comment on the advance notice of proposed rulemaking published by the U.S. Department of Commerce, Bureau of Industry and Security (“BIS”) on Nov. 19, 2018 (83 Fed. Reg. 58201) concerning proposed criteria for identifying emerging technologies that are essential to U.S. national security (the “ANPRM”).

Please note that the views expressed herein are being presented only on behalf of the Section. They have not been approved by the House of Delegates or the Board of Governors of the ABA, and accordingly, they should not be construed as representing the policy of the American Bar Association.

In the ANPRM, BIS states that it welcomes comments on the following issues: (1) how to define emerging technology to assist identification of such technology in the future; (2) criteria to apply to determine whether there are specific technologies within these general categories that are important to U.S. national security; (3) sources to identify such technologies; (4) other general technology categories that warrant review to identify emerging technologies that are essential to U.S. national security; (5) the status of development of these technologies in the United States and other countries; (6) the impact specific emerging technology controls would have on U.S. technological leadership; and (7) any other approaches to the issue of identifying emerging technologies important to U.S. national security, including the stage of development or maturity level of an emerging technology that would warrant consideration for export control. The Section’s comments on these issues are set forth below.
EXECUTIVE SUMMARY

In the Section’s view, it is imperative that BIS seek to develop criteria for identifying emerging technologies that are essential to U.S. national security in ways that are consistent with both the Export Control Reform Act of 2018 (the “ECRA”) and the Foreign Investment Risk Review Modernization Act of 2018 (the “FIRRMA”), which were concurrently enacted via the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (the “NDAA”). Towards this end, the Section proposes that BIS consider defining the term “emerging technologies” in the following manner:

“Emerging technologies” are specific, non-mature technologies that:

1. are important for the United States in maintaining a qualitative military or intelligence advantage or for U.S. national security;
2. are not widely available or traded within the global marketplace;
3. are not available in US embargoed countries including arms embargoed countries;
4. do not possess significant commercial value to US persons who have invested in making the finished items and technology generally available commercially; and
5. cannot be controlled or monitored through other methods.

This proposed definition is narrowly tailored, salient, useful, effective, flexible, and balanced.

Noting that the ECRA requires that an interagency process be used to identify emerging technologies that are essential to U.S. national security, the Section recommends that BIS reach out to all appropriate offices and bureaus of the cognizant federal agencies and to require them to evaluate things using the definition for “emerging technologies” proposed by the Section or one similar to it. During the review process, the Section also urges BIS to seek input from technical advisory committees and companies and other entities (e.g., universities and venture capital investment firms) that are believed to be working or involved in any of the 14 technology categories that are identified in the ANPRM and should take into account foreign availability of emerging technologies. In addition, the Section suggests that BIS should consider proposing controls on emerging technologies through multilateral regimes to ensure that the controls are effective, and that they do not result in unilateral controls on U.S. industry that have the effect of negatively impacting U.S. leadership in the relevant sectors by facilitating development outside the United States in the void created by unilateral controls on U.S. exports.

COMMENTS

Before beginning to address the specific issues for which BIS is seeking comments, the Section believes that it is important to note that the concurrent enactment of FIRRMA and the ECRA via the NDAA reflected a compromise. Congress decided that measures it sought to improve protection of U.S. national security would not all be placed in the FIRRMA, but would instead be divided between FIRRMA and the ECRA. The two statutes, however, remain interrelated. The FIRRMA enhances the ability of the Committee on Foreign Investment in the United States (the
“Committee” or “CFIUS”) to control inbound investments that might threaten U.S. national security. The ECRA enhances the ability of the federal government to control outbound transfers and in-country releases to foreign nationals of commodities, materials, software, and technology.

The FIRRMA and the ECRA pursue some of the same objectives, including: protect U.S. national security and so do, in party, by addressing threats to diminish, blunt, or neutralize any of its significant military or intelligence advantages or to thwart its pursuit of foreign policy objectives. Such threats have recently increased. As the FIRRMMA explains:

“It is the sense of Congress that – …

the national security landscape has shifted in recent years, and so has the nature of the investments that pose the greatest potential risk to national security …

[T]he President should lead a collaborative effort with allies and partners of the United States to strengthen the multilateral export control regime”1

As will be discussed below, BIS can play a critical role in contributing to the realization of such objectives by carefully analyzing emerging technologies.

1. **How to Define Emerging Technology**

Significantly, the term “emerging technology” is not defined in the FIRRMA or the ECRA. Given this fact, the Section offers the following recommendations on how BIS should define emerging technology.

Firstly, a definition for “emerging technology” should be circumscribed. Beginning in the early 1970s—before entering the consumer marketplace in the mid-1980s—cellular-phone technology was “emerging” yet unlikely to be viewed as a potential national security threat. However, as exemplified during recent conflicts in Iraq and Afghanistan, the use of cellular technology did pose a security threat via its use to trigger improvised explosive devices (IEDs). The use of commercial airliners in the attacks on 9/11 also illustrates the use of technology that was once “emergent” (i.e., jet aircraft). Similarly, commercially available information technology (IT)—that was once defined as “emergent”—is now regularly used for information “hacking” and for disrupting sensitive information technology systems (e.g., cyberattacks). These examples all illustrate the metamorphosis of prior “emerging technologies” that ultimately posed some form of national security threat (i.e., “asymmetric”) to the United States. However, restricting the development of cellular communications, jet aircraft, and computers—when nascent or “emerging”—would have been against the larger commercial interests of the United States.

Tailoring emerging technology controls narrowly to avoid adverse impact on the development of the commercial technologies in the US is consistent with Section 1758 of the ECRA which requires that the inter-agency process take into account “the effect export controls imposed pursuant to this section may have on the development of such technologies in the United States.” It is also

1 FIRRMA, §1701(b)(4) and (7).
consistent with ECRA’s stated exception that the Secretary of Commerce shall not require a license in cases where a US person “generally makes the finished item and associated technology available to its customers, distributors, or resellers.” Therefore, for purposes of proposing a revised definition of the term “emerging technology,” it would seem reasonable that the term should be both narrowly tailored to avoid economic overreach that could damage U.S. interests in making commercial sales of generally available products such as (historically) cell phones and commercial aircraft and focus primarily on conventional military force and related concerns.

A second factor in support of a circumscribed “emerging technology” definition is the increasing influence and importance of global trade and commerce. Business and industry—and the associated development of new technologies within various sectors—is increasingly reliant on cross-border transactions that involve frequent exchanges of human and financial capital, information, and intellectual property. Supply chains are increasingly reliant on non-US sources of supply as are the design, assembly, and delivery of products and services. Further, this global trade reality has only increased the pace by which new technologies are developed, improved, and offered within the broader marketplace, as increasing global competition has spurred innovation in the race for competitive advantage. Therefore, increased regulatory hurdles and overly broad technology restrictions (driven by national security “protections” and placed on US industry) may hamper global commerce and US economic competitiveness within that global marketplace. Taking into account non-US sources of supply in determining whether to regulate an emerging technology is consistent with Section 1758 of ECRA which requires that the inter-agency process take into account “the development of emerging and foundational technologies in foreign countries.” There is no need to control a technology that is already widely available in the global marketplace.

This leads logically to a third factor. Section 1758 of ECRA also requires that the inter-agency process take into account “the effectiveness of export controls imposed pursuant to this section on limiting the proliferation of emerging and foundational technologies to foreign countries.” ECRA also requires, at a minimum, that licenses be required to export, reexport or in-country transfer of controlled emerging technologies to countries that are subject to US embargoes including arms embargoes. If a technology is already present, or being developed, in a US embargoed country, it would not be effective to impose US export control under ECRA to that technology. Thus, foreign availability of the technology in a US embargoed country should weigh against the imposition of controls on that technology.

Therefore, the following characteristics may be recommended when crafting an appropriate definition of “emerging technologies”:

- Limited: narrowly tailored
- Salient: focus on symmetric / conventional force impact
- Balanced: considers global commercial and economic interests of the United States
- Effective: avoids controlling technology that is “published” (per 15 CFR 734.7) or that is already present in US embargoed countries
- Flexible: awareness of the increasing pace of technological advancements
- Useful: can objectives (such as intelligence collection) be more effective from other sources
In light of the above, the following definition of “emerging technologies” is proposed:

“Emerging technologies” are specific, non-mature technologies that:

6. are important for the United States in maintaining a qualitative military or intelligence advantage or for U.S. national security;
7. are not widely available or traded within the global marketplace;
8. are not available in US embargoed countries including arms embargoed countries;
9. do not possess significant commercial value to US persons who have invested in making the finished items and technology generally available commercially; and
10. cannot be controlled or monitored through other methods.

2. Criteria to Be Used in Making Emerging Technology Determinations

In terms of determining which technologies within the “emerging technology” definition proposed above are important to U.S. national security, it may be advisable to generate a series of questions that require qualitative and quantitative evidence. For example (and without limitation), such questions could include:

- Is the technology nascent or does it significantly innovate on existing capabilities?
- Does the technology materially advantage US military or intelligence capabilities?
- Is the technology available or is it being developed internationally?
- Is technology development limited to a finite number of public or private organizations principally within the United States or within the United States or its major allies?
- Is the technology being developed commercially?
- Could the technology have significant civil or commercial utility?
- Is the technology expected to be marketed and sold within the global marketplace?
- Is the technology “published” (per 15 CFR 734.7) and therefore not possible to control?
- Is the technology available or being developed in US embargoed countries including arms embargoed countries?
- Can the technology be defined based on clear criteria that will allow for its control with precision?
- Would technology restrictions have a materially negative impact to US commercial interests?
- Would the technology be better controlled if the controls were associated with specific problematic end uses (e.g., WMD proliferation or terrorism end uses)?

3. Sources That Can Be Used to Identify Emerging Technologies

Pursuant to Section 109 of the ECRA, BIS is required to “draw upon the expertise, resources, and equities of all relevant United States Government agencies, industries, and academic institutions
to identify and describe such emerging critical technologies.” In light of this requirement, the
Section offers the following recommendations.

First, as part of interagency discussions, BIS should make sure to engage with the appropriate
offices and bureaus at the cognizant federal agencies. For example, the U.S. Department of
Defense (“DoD”) works with U.S. companies and universities in the development of emerging
technologies through the Defense Advanced Research Projects Agency (“DARPA”). Similarly,
the U.S. Department of Energy (“DoE”) and NASA have offices that will engage with U.S.
companies and universities for similar projects. In addition, the venture capital investment entities
supporting the intelligence and defense community (such as InQTel and DIU) are valuable sources
of information with respect to potential new emerging technologies. As such, when engaging in
interagency discussions, BIS should seek to ensure that it reaches out to these and other appropriate
federal government stakeholders, including (among others): the U.S. Department of State (“DoS”),
the intelligence agencies, and the U.S. Patent and Trademark Office (“PTO”).

Second, the U.S. Department of Commerce (“DoC”) should continue with its plans to establish a
Technical Advisory Committee on emerging technologies. This TAC should include
representatives from universities, laboratories, corporations, venture capital firms, and other
entities that work with or advise cutting-edge technology companies.

Third, it may be beneficial for BIS to consider making confidential visits to certain companies
that BIS believes work in some of the 14 categories identified in the ANPRM. This would be an
opportunity to learn more about the technologies firsthand.

Finally, BIS should do all that it can to stay informed of the latest developments relating to
emerging technologies. Towards this end, BIS should regularly read materials on developments
in emerging technologies, such as reports that are issued by leading think tanks and articles that
appear in well-respected magazines such as *WIRED*.

4. **Other General Technology Categories That May Warrant Review**

In the ANPRM, BIS identified 14 “representative general categories of technology for which
Commerce currently seeks to determine whether there are specific emerging technologies that are
essential to the national security of the United States.” Although subject to the EAR, those
categories of technology are only regulated for control in limited circumstances such as “to
embargoed countries, countries designated as supporters of international terrorism, and restricted
end uses or end users.” The categories present a “representative list of the technology categories
from which Commerce, through an interagency process, seeks to determine whether there are
specific emerging technologies that are important to the national security of the United States for
which effective controls can be implemented that avoid negatively impacting U.S. leadership in
the science, technology, engineering, and manufacturing sectors.”

BIS also stated in the ANPRM that it would welcome comments on “other general technology
categories that warrant review to identify emerging technology that are important to U.S. national
security.” To that end, the Section recommends that BIS consider the possible addition of “energy
storage technology” to its list of general categories of technology to identify emerging technologies essential to United States national security.

Energy security is plainly an essential part of the national security of the United States. At the heart of future energy security is energy storage technology. For example, in Fall 2018, the DoE recognized the importance of energy security and the emerging role of energy storage technology through renewal of funding for the Joint Center for Energy Storage Research (JCESR), an effort led by the Argonne National Laboratory and focused on advancing energy storage technology. Such energy storage technologies include advanced battery materials, superconducting magnet energy storage systems, and many more. As described by the Director of the JCESR:

“This is a storage moment. Electric cars, grid storage, and battery-powered planes are creating a market that is exploding. To meet this market demand requires a diversity of batteries that can be applied for a diversity of uses. In JCESR, our researchers are designing transformative materials atom-by-atom and molecule-by-molecule, getting us that much closer to the U.S. leading this important market transformation.”

See https://www.jcesr.org/. Whether effective export controls can and should be implemented for certain energy storage systems is an open issue subject to substantial question. Nonetheless, in light of the centrality of certain emerging energy storage technology to the future industrial base and economy of the United States, the Commerce, Energy, Defense and other Departments through the interagency process should assess whether certain emerging energy storage technologies are essential to the national security of the United States taking into account the criteria set forth in 2 above.

5. The Potential Impact of Emerging Technology Controls on U.S. Companies

In the ANPRM, BIS identified the goal of determining whether there are specific emerging technologies that are important to the national security of the United States for which effective controls can be implemented that avoid negatively impacting U.S. leadership in the science, technology, engineering, and manufacturing sectors. BIS further correctly noted that any new U.S. unilateral controls could run the risk of allowing other countries to advance in these critical technology areas at the expense of leadership of U.S. industry. Thus, any review should take into account foreign availability of emerging technologies.

If such technologies are readily available abroad, or will be readily available in the near term, this would be an important factor of whether to impose unilateral controls, and if so, the limitations on such controls. To the extent such emerging technologies are not in an area where the U.S. has a distinct lead, Commerce should consider the benefits and disadvantages of implementing unilateral controls on such technologies.

Commerce should also consider proposing controls through the multilateral regimes to ensure that the controls are effective, and do not result in unilateral controls on U.S. industry that have the effect of negatively impacting U.S. leadership in the relevant sectors by facilitating development outside the U.S. in the void created by unilateral controls on U.S. exports.
6. **Other Approaches to Identifying Emerging Technologies and Their Development Status**

The regulatory effort to address the “shift” in the national security landscape that has occurred in recent years and is alluded to in the FIRRMA and the ECRA dates back to April 2013 when BIS promulgated a final rule a new Export Control Classification Number (“ECCN”) series, 0Y521, on the Commerce Control List (“CCL”). As BIS explained in that final rule:

> “Items will be added to the 0Y521 ECCNs by the Department of Commerce, with the concurrence of the Departments of Defense and State, when it identifies an item that should be controlled because it provides a significant military or intelligence advantage to the United States or because foreign policy reasons justify such control.”

Unlike other ECCN series, which classify an item’s technical characteristics, the 0Y521 ECCNs reflected the view that such items, had to be controlled at the outset because, in all likelihood, an attempt to control them subsequently would be too late. In the digital era, the item, software, related know-how, and technology would proliferate to U.S. adversaries. The adoption of the 0Y521 ECCNs implemented a strategy that can be described as apply restrictive unilateral control at the outset. Any commodity, material, software, or technology parked in 0Y521 ECCN was to be “subject to a nearly worldwide license requirement (i.e., for every country except Canada) with a case-by-case license review policy, through regional stability (RS Column 1) controls.”

The case-by-case license review would determine whether:

> “export or reexport could contribute directly or indirectly to any country’s military capabilities in a manner that would destabilize a region’s military balance contrary to the foreign policy interests of the United States.”

Few entries have been made to the 0Y521 ECCNs. One entry, made on August 8, 2016, reflected an apparent concern with the use of tritium for nuclear weapons development and production. BIS issued an interim final rule to classify certain:

> “specified targets ‘specially designed’ for the production of tritium and related ‘development’ and production’ technology under Export Control Classification Numbers (ECCNs 0A521 and 0E521, respectively, on the Commerce Control List (CCL)).”

BIS subsequently removed the “specified targets” from the 0Y521 series.

---

3 *Id.* at 22192.
4 *Id.* [Emphasis added.]
5 BIS, *Amendment to the Export Administration regulations To Add Targets for the Production of Tritium and Related Development and Production Technology to the List of 0Y521 Series*, Federal Register, Vol. 81, No. 152, August 8, 2016, p. 52326.
Such 0Y521 ECCN classifications appear to suggest that BIS only used such determinations in rare and extraordinary cases and only for relatively short time periods.

To protect U.S. national security would appear to require that the U.S. revise its approach to the issue of “identifying emerging technologies.” We discuss some of those ways in a Part 6.B below. Before doing so, however, we think it important to highlight the relationship between “identifying emerging technologies” and the enhancement of the CFIUS review process by FIRMA and the FIRRMA-related Pilot Program that was announced by the Treasury Department in October 2018.

A. Relationship of “Emerging Technologies” to the FIRRMA-Related Pilot Program

Enactment of the FIRRMA expanded the authorities of the President and CFIUS under Section 721 of the Defense Production Act of 1950 (the “DPA”) to review certain foreign direct investments in certain covered transactions involving U.S. entities. Among other things, the FIRRMA expanded the scope of foreign investments in the United States that would be subject to national security review pursuant to Section 721 of the DPA.

In accordance with powers granted by the FIRRMA, the Treasury Department issued interim regulations to establish the FIRRMA-Related Pilot Program on October 11, 2018 (the “Pilot Program Regulations”). Pursuant to the Pilot Program Regulations, which took effect on November 10, 2018, parties to a “pilot program covered transaction” are required to notify CFIUS of the transaction. Under the Pilot Program Regulations, a “pilot program covered transaction” is defined as either any “pilot program covered investment” or “any transaction by or with any foreign person that could result in foreign control of any pilot program U.S. business, including such a transaction carried out through a joint venture.”

The Pilot Program Regulations define “pilot program U.S. business” to mean:

“any U.S. business that produces, designs, tests, manufactures, fabricates, or develops a critical technology that is:

(a) Utilized in connection with the U.S. business’s activity in one or more pilot program industries; or

(b) Designed by the U.S. business specifically for use in one or more pilot program industries.”

The Pilot Program Regulations define “pilot program covered investment” to mean:

“an investment, direct or indirect, by a foreign person in an unaffiliated pilot program U.S. business that could not result in control by a foreign person of a pilot program U.S. business and that affords the foreign person:

7 31 CFR §801.213. [Emphasis added.]
(a) Access to any material nonpublic technical information in the possession of the pilot program U.S. business;

(b) Membership or observer rights on the board of directors … of the pilot program U.S. business or the right to nominate an individual to a position on the board …[of such business]; or

(c) Any involvement, other than through voting of shares, in substantive decisionmaking of the pilot program U.S. business regarding the use, development, acquisition, or release of critical technology.”

The definition of “critical technologies” set forth under Section 801.204 of the Pilot Program Regulations tracks with the definition of that same term enumerated under Section 1703 of the FIRRMA to consist of the following six categories:

1. Defense articles and services included on the U.S. Munitions List set forth in the International Traffic in Arms Regulations (“ITAR”);

2. Items included on the CCL set forth in Supplement No. 1 to part 774 of the EAR;

3. Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology (relating to export and import of nuclear equipment and material);

4. Nuclear facilities, equipment, and material covered by 10 CFR part 110;

5. Select agents and toxins covered by 7 CFR part 331, 9 CFR part 121, or 42 CFR part 73;

6. **Emerging and foundational technologies** controlled pursuant to section 1758 of the ECRA.9

The sixth category provides a clear linkage between FIRRMA and ECRA. FIRRMA’s pilot program regulations applies to parties to a “pilot program covered transaction.” One subset of such transactions are those in which the investment would afford the foreign person “involvement, other than through voting of shares, in substantive decisionmaking” in the target business regarding the “use, development, acquisition, or release of critical technology.” And “critical technology” includes “emerging and foundational technologies.” Since BIS has, however, treated “emerging technologies” separately from “foundational technologies,” we omit “foundational” from this discussion.

Section 1758 of the ECRA provides for an interagency process to identify “emerging technologies” that are “essential” to U.S. national security and that are not critical technologies described in

---

8 31 CFR §801.209. [Emphases added.]

9 31 CFR §801.204. [Emphasis added.]
clauses (i) through (v) of the DPA §721(a)(6)(A). The interagency process is to draw upon multiple sources, identified in Section 1758, including two that will consist of advisory committees established by the Secretary of Treasury and that will focus, in part, on foreign country efforts to develop emerging technologies: “(i) the development of emerging … technologies in foreign countries; … and (iii) the effectiveness of export controls imposed … on limiting the proliferation of emerging technologies to foreign countries.”

Furthermore, the quoted provision also requires BIS to determine if it can effectively control and thereby limit the proliferation of the “emerging technologies” to foreign countries. It would be reasonable to interpret that provision as aiming to deny exports of “emerging technologies” to U.S. adversaries, to countries that would re-export them to such adversaries, but to encourage exports to allies that might facilitate the U.S. objective to gain or maintain leadership in development of such emerging technologies.

B. Possible Ways of Identifying Emerging Technologies

We note that pursuant to section 1703 of the NDAA, the chairperson of CFIUS “may recommend [emerging and foundational] technologies for identification under the interagency process set forth in section 1758(a)” of the ECRA and that such recommendations by the chairperson shall be informed by reviews and investigations conducted by the Committee, as well as non-notified and non-declared transactions identified by the Committee. The identification of such emerging technologies, pursuant to section 1758(a) of the ECRA, shall further be informed by publicly available information, classified information, and information provided by the advisory committees established by the Secretary to advise the Under Secretary of Commerce for Industry and Security, including the Emerging Technology and Research Advisory Committee. We further note that, in section 225 of the NDAA, the Under Secretary of Defense for Research and Engineering has been mandated to prescribe “procedures for rapid reaction to emerging technology” which includes “a process for making investment determinations” in identified significant and emerging technologies. We expect that the approach of the interagency process for identifying emerging and foundational technologies will therefore be informed the (potentially classified) information ascertained by means of the section 225 process.

As stated in the ANPRM, once an emerging or foundational technology has been identified, the Act authorizes Commerce to establish controls, including interim controls, on the export, reexport, or transfer (in country) of that technology, and in determining the appropriate level of export controls, the Department must consider the potential end-uses and end-users of the technology, and countries to which exports from the United States are restricted (e.g., embargoed countries), and at a minimum must require a license for the export of emerging and foundational technologies to countries subject to a U.S. embargo, including those subject to an arms embargo.

With respect, therefore, to the request for comments on “approaches to the issue of identifying emerging technologies important to U.S. national security, including the stage of development or maturity level of an emerging technology that would warrant consideration for export control”, we suggest that an approach that is reflective of, and closely tied to, the innovation and development

---

10 ECRA, §1758(a)(2)(B)(i) and (iii).
cycle in the U.S. scientific and start-up communities, would be most effective for the timely and appropriate identification and evaluation of emerging technologies.

The object of such an approach would be to create a metric to permit identification of an emerging technology at a point after it has in fact emerged as a true technology within the meaning of the EAR, but before it has been exploited and widely internationally disseminated via licensing or joint development agreements, such that there is no longer significant value in implementing unilateral or multilateral export controls with respect to the technology.

In the United States, there may be several avenues to the refinement and eventual successful commercial exploitation of a truly new or emerging technology. One important pathway, however, follows a common general pattern and is significant for the consideration of BIS as it establishes an approach to identification of future emerging technologies. In this pathway, the following general stages occur:

a. University-located, U.S. government-funded “fundamental research” is undertaken by one or more U.S. or foreign national principal investigators, resulting in technology which is “published” and therefore not subject to the EAR.

b. The principal investigators form a U.S. entity and license certain aspects of the published technology from the University. In many cases, initial “friends and family” funding is obtained from the personal network of the principal investigators; this may include foreign sources of funding, including strategic funders who may also be linked to foreign government interests. In some cases, additional grant funding is obtained through innovation competitions which are often ultimately U.S.-government funded. It may already be at this stage that significant aspects of technological development and research approaches are shared with these early funders, as a sign of good faith or in order to comply with contractual obligations.

c. After substantial refinement of the initially licensed technology with a view to commercial viability, the U.S. entity has identified the most promising avenues of its technology for commercial exploitation, and is able to attract a so-called “seed series” round of investment. This would typically involve more seasoned funding sources, with higher expectations of involvement in the entity at a formal level, including board seats and potentially involvement in the strategic direction of the company. This grooming period sets the stage for the next funding round: the Series A round.

d. The Series A financing will used to scale up the entity’s operations, prepare for commercial production and serious sales and marketing efforts, and may often be targeted to investors who may wish to use the entity’s technology in a strategic manner for their own industrial group’s development. The company’s governance, board, and business plan will be formalized and subject to intensive review (including for export control and CFIUS risk) by the investor counsel. Key strategic decisions including corporate restructuring, offshoring
of IP, licensing and joint development agreements with industry partners, and the like are often considered at this stage and heavily influenced by the new board and investors. Following the Series A financing, if financial viability continues, is often considered the stage at which a startup becomes a “mid-stage” company. At this point, the viability of the entity’s technology is typically not in question, but rather whether or not it may be successfully commercialized.

We believe that a BIS approach to identifying emerging technologies that does not facilitate identification in the pre-commercial-viability stage (between the steps C and D described above) risks only identifying such technologies after imposing export controls would no longer promote U.S. national security nor protect the U.S. commercial and innovative advantage with respect to such technologies.

Moreover, the current EAR approach appears to still be based in assumptions that were more appropriate and reasonable when government military and aerospace agencies tended to take the lead in the development of new technologies and provided “spin offs” of such technologies for commercialization. The government is seldom the locus of lead development of emerging technologies and is struggling to convince Silicon Valley firms to share their expertise and discoveries with the government for protection of U.S. national security.

The current innovation and national security landscape is one in which the speed of development-to-deployment may determine who will gain the ultimate advantage from the new technology. Speed has become the “differentiating factor” — a point emphasized by the Under Secretary of Defense for Research and Engineering, in testimony before the U.S. Senate Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities, on April 18, 2018:

“We are in constant competition, and the pace of that competition is increasing. In a world where everyone pretty much today has equal access to technology, innovation is important, and it will always be important, but speed becomes the differentiating factor. How quickly we can translate technology into fielded capability is where we can achieve and maintain our technology edge. It is not just about speed of discovery. It is about speed of delivery to the field.”

Consequently, a consideration of a shift in the timing of when to identify an emerging technology may be as important as how to identify an emerging technology, in order to strike a balance between permitting U.S. industry to reap the economic benefits of innovation without forfeiting the race to field technology to a military adversary. By the time that a technology might be well-recognized enough to be dubbed “emerging” or recognized as having a potential to be a “critical technology,” it may be too late for application of controls to prevent an adversary from gaining

---

knowledge of its existence and, through strategic investment in a start-up, from gaining detailed technical data and know-how about it.

In addition, waiting until a new technology gains public recognition as an “emerging or foundational technology” (and, by definition in ECRA as a “critical technology”) may put the U.S. government at odds with U.S. industry. The government may belatedly discover a need to control a new technology because it sees it as a “critical technology” by that time, however, U.S. industry may have invested heavily in its development have structured their business in such a way that the imposition of new export controls requiring licensing for the export or reexport of the relevant commodity, materials, software, or technology would be a critical blow to economic competitiveness. Moreover, if the government only applies export controls at this later stage, U.S. adversaries may have already exfiltrated key technical data because the U.S. companies did not take the precautions and safeguards that export controls would have required.

An effective approach for the identification of emerging technologies, therefore, should consider the following factors:

1. Whether the technology under consideration has reached the point of development at which it in fact has been refined sufficiently to constitute technology within the meaning of the EAR (namely, that it is “information necessary for the “development,” “production,” or “use” ..of an item [which could itself be subject to controls]);

2. Whether the technology has yet been refined to the point that it has become a viable target for investment by angel, venture capital, fund, or other investors (e.g., subject of a Series A financing round, in the context of a startup company);

3. Whether the technology is one for which there exists redundancy of commercially exploitable avenues of availability outside of the United States and Country Group A;

4. Whether U.S. intelligence sources find that a foreign adversary has targeted and made efforts to gain access to a technology that is under commercial development at a company (including start-ups) or that is the subject of fundamental research;

5. Whether U.S. intelligence sources find that a foreign adversary is investing in the development of the technology at a state-owned or state-sponsored research facility that is known for transferring its discoveries to the adversary’s military, or is moving more swiftly than the U.S. to deploy the technology for military or intelligence purposes. As a DoD guide to intellectual property, published back in October 2001 observed:

   “In the past, research programs funded by the Department of Defense (DoD) often led industry efforts in technology. Today [2001] the reverse is largely the case – technology leadership has shifted to
industry, where most research and development (R&D) dollars are spent. …  

Challenges to the Government today are to find ways to entice commercial industry into collaborating with the Department in vital research efforts …”\(^\text{12}\)

6. In addition, since a distinguishing criterion of “fundamental research” is whether or not the research is intended for eventual publication, the BIS may wish to consider recommending for interagency consideration whether certain government-supplied funding should make clear that “publication” of the results can only be intended after a government review of the results (similar to a review of a patent application to determine if it should be placed under a secrecy order).

* * * * *

Your consideration of our comments is greatly appreciated. Please let us know if it would be beneficial for us to meet with you and other BIS officials to elaborate on our recommendations, which we would be pleased to do.

Respectfully submitted,

Robert L. Brown  
Chair, ABA Section of International Law