ITI Response to the Advance Notice of Proposed Rulemaking for the Identification and Review of Control for Certain Foundational Technologies (BIS-2020-0029)

November 9, 2020

Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
1401 Constitution Avenue, NW
Washington, DC 20230

Re: Identification and Review of Controls for Certain Foundational Technologies (BIS-2020-0029)

The Information Technology Industry Council (ITI) represents the global voice of the tech sector, advocating for policies that advance U.S. leadership in technology, promote innovation, open access to new and emerging markets, protect consumer choice and privacy, enhance trust in technology, and foster increased global growth. Our membership includes more than 70 high-tech and tech-enabled companies, including wireless and wireline network equipment providers, computer hardware and software companies, internet and digital service providers, mobile computing and communications device manufacturers, consumer electronics companies, payment networks and network security providers. All of our members are headquartered, operate U.S. subsidiaries, or otherwise have significant operations in the United States, and their investments have propelled economic growth and innovation across the country.

ITI appreciates the opportunity to provide comments in response to the Advance Notice of Proposed Rulemaking (ANPRM) regarding the Identification and Review of Controls for Certain Foundational Technologies. We recognize that concerns about U.S. national security are at the heart of this ANPRM. We also want to thank the Bureau of Industry and Security (BIS) for acknowledging our previous concerns about short comment periods and deciding to administer what has been extended to a 75-day comment period. This longer window allows for the development of significantly more substantive and comprehensive comments in response to BIS’s inquiries. Additionally, we welcome the recent introduction by BIS of a confidential process that safeguards information provided by industry participants in response to such requests to avoid the disclosure of business proprietary or confidential information.

U.S. Technological Leadership Matters for U.S. National Security
Companies in the United States have long spearheaded the development of the most innovative and cutting-edge technologies, transforming the global economy and catalyzing tremendous growth for the United States. The U.S. innovation ecosystem has also benefitted from the significant contributions of U.S. subsidiaries, which in 2016 accounted for 16 percent of total...
business research and development (R&D) spending in the United States. Today, other nations and companies are competing to find the next major advancement. In some cases, competitors go to great lengths to gain dominance, particularly in the area of science and technology development.

U.S. national security depends on continued U.S. technological leadership. This leadership drives U.S. innovation, job creation, and economic growth. Remaining at the cutting edge of developing and commercializing technologies will ensure they are available to the private sector and the defense industrial base. Indeed, Congress and the President recognized in the Export Control Reform Act (ECRA) that “[the] national security of the United States requires that the United States maintain its leadership in the science, technology, engineering, and manufacturing sectors.” The statute further emphasizes that any proposal to introduce controls on technology must take into account potential impacts to the future of U.S. technological leadership.

ITI is concerned that overly broad controls on technology products will undermine and limit the ability of companies to participate in the global marketplace, which will in turn disrupt the virtuous cycle of private-sector R&D investments made possible by revenues from sales of U.S. products to a diverse customer base in overseas markets.

Accordingly, the implementation of any new export control architecture must be informed by a comprehensive assessment of the threat landscape and a distinct understanding of the specific and clearly articulated national security objectives that are intended to be achieved. While the private sector can provide important understandings of market dynamics, U.S. intelligence agencies also must be involved to make a determination about the impact of a particular control measure and its necessity to U.S. national security – it must be fully risk-informed.

ITI and its member companies understand the national security concerns of the U.S. government. However, the overly broad, unilateral control of technologies will result in limiting U.S. companies’ global competitiveness and their ability to lead in the development of core technologies. Given the desire of the Administration and Congress to ensure that U.S. companies remain among the most innovative and competitive in the world, a balanced and thorough review of technologies identified for export control is essential.

By definition, foundational technologies are already mature and widely available. Imposing additional controls on foundational technologies could hinder the United States from attracting the world’s top talent, necessitate the costly reconfiguration of global supply chains and R&D networks, slow economic growth, and invite speculation about the reliability of U.S. partners and suppliers. All these outcomes hurt U.S. technological leadership, which paradoxically undermines U.S. national security. It is therefore our view that, unless any new controls meet the rigorous thresholds established in ECRA and outlined in our comment, new restrictions on technologies based on their “foundational” status are unnecessary, will be ineffective in limiting the global development and proliferation of these already-ubiquitous technologies, and ultimately undermine short- and long-term U.S. national security objectives.

Process Considerations
As BIS promulgates rules to identify foundational technologies as well as emerging technologies, ITI puts forth several process considerations to help ensure that any ensuing controls are tailored, effective, and feasible to implement from a compliance perspective. We cannot stress enough that facilitating robust stakeholder engagement throughout the lifespan of these controls will be absolutely critical, especially when evaluating potential impacts to the U.S. technology industry’s competitive edge. Accordingly, we have outlined several priority process considerations for the identification, implementation, and ongoing evaluation of “foundational technologies.”

We also note that any expansion of the export control regime will necessitate additional resources to ensure adequate implementation and enforcement. We recommend that the Secretary of Commerce request, and Congress provide, additional resources to support the continuous review of U.S. export controls. As the Department of Commerce promulgates rulemaking(s) to implement ECRA and other export control-related mechanisms, it would be helpful for it to evaluate resource requirements to manage the new regime and communicate those requirements to relevant stakeholders.

Identifying New Technologies for Control
We urge BIS to pursue individual rulemaking processes for each new control under consideration and to do so through public notice-and-comment processes with sufficient comment periods lasting at least 60 days. Taking this procedural approach to identifying new technologies for control will support the robust and substantive engagement with stakeholders that is fundamental to implementing effective controls.

As noted in the introduction, we welcome BIS’s decision to establish a process for accepting confidential submissions for sensitive and proprietary business information. We encourage BIS to extend this process to all future rulemakings and proposed controls to ensure that BIS can benefit from the full range of the U.S. business community’s expertise.

Implementing New Controls
Except as required by ECRA, existing license exceptions, exclusions, or authorizations should apply to any controls on “foundational technologies.” In addition, BIS must use license exceptions or other mechanisms to allow for unrestricted intracompany exports, re-exports, and transfers between and amongst U.S. companies, subsidiaries, and non-U.S. counterparts. BIS should also provide an exception for intracompany deemed exports to foreign national employees of U.S. operations and their non-U.S. subsidiaries. In section 4565(a)(4)(B)(iii) of the Foreign Investment Risk Review Modernization Act (FIRRMA), policymakers indicated that transactions among affiliates were not an area of concern. BIS’s rulemaking should reflect the outcome reached in FIRRMA as this approach would limit disruption to a company’s global supply chains and R&D activities.

Along those same lines, BIS should specify that all technologies currently available overseas are deemed compliant upon the effective date for new controls as well as establish a transition or “safe harbor” period for companies to implement new controls. This transition period is especially important given the lengthy amount of lead time it can frequently take to obtain licenses. The length of time for any such period should be determined in consultation with industry stakeholders, especially as the appropriate length may vary depending on the specific control. Finally, the structure of any future controls should be consistent with that of the Export Administration
Regulations (EAR), and technologies should be identified through Export Control Classification Numbers (ECCNs) in order to facilitate effective compliance.

Providing for the Modification and/or Removal of Controls
Identified technologies that meet the statutory requirements should be subject to unilateral controls only in cases of exclusive development and availability in the U.S. market. Any such controls should be removed once that exclusivity no longer exists.

As such, we recommend that BIS spell out in detail the procedures for how it intends for an “ongoing interagency process” to identify and evaluate controls to be modified or removed from the lists altogether. For example, BIS should consider establishing a mechanism by which stakeholders can petition for the removal of controls based on new information, such as a change in foreign sourcing, technological advancements, etc. An additional aspect could be establishing a schedule for the initiation of a new interagency review to evaluate both the effectiveness of the control as well as whether the conditions that led to the addition of the control are still relevant. The “ongoing interagency process” would also benefit from systems intended to constantly reevaluate the state of the initial conditions, including specific opportunities for industry engagement and feedback. As part of that, we strongly encourage BIS to take advantage of industry expertise within the technical advisory committees, including the Emerging Technology Technical Advisory Committee. We are concerned that once technologies are added to the control list, it will be difficult to remove them, even if they no longer meet the standards established pursuant to this process. Considering the rapid pace of technological advancement, this point is especially relevant to the current rulemaking.

Principles for Controlling Foundational Technologies
While many of these principles were included in ITI’s January 2019 submission to the ANPRM for emerging technologies, the stakes of overcontrolling foundational technologies are even higher for the continued success of U.S. industrial leadership because, by their definition, foundational technologies are already widely available and any ensuing controls would likely mean the immediate disruption of ongoing R&D and production activities. ITI has compiled several principles as well as identified areas of concern that are relevant to the current ANPRM.

Current Export Controls Policy Environment
There have been more than 500 additions to the Entity List since January 2017, in addition to many other changes or proposed changes to the U.S. export control regime. This observation should not be construed as criticism of any individual control, but instead as an indication of the operational challenges facing corporate compliance departments due to the sheer volume of controls. As these departments work to keep pace with the changing landscape, they are increasingly devoting more and more of companies’ limited resource pools to compliance, spending dollars and time that could be more constructively channeled towards advancing technological developments. BIS should consider the cumulative impact of the U.S. export control regime on the U.S. technology industry as it evaluates how best to address specific risks to U.S. national security, especially as relates to the value of using existing authorities as opposed to introducing controls under new authorities. BIS should also consider effective and efficient approaches to controls that utilize smart technology and can be leveraged across authorities.

The Detrimental Impact of Unilateral Controls

Avoiding unilateral controls is imperative to ensuring U.S. leadership on innovative technologies. In cases where there is foreign availability in terms of comparable quality, quantity, and cost, a unilateral control will be ineffective in preventing end users of concern from acquiring the controlled technology. And, as noted in a report by the President’s Council of Advisors on Science and Technology, “when it acts unilaterally, the United States often raises suspicions (however ill-founded) among allies that it is motivated by economic-competitiveness concerns, rather than by national security.”

Unilateral export controls imposed on widely available technologies cause direct, and possibly irrevocable, harm to companies in the United States that are subject to the control. If the scope of the controls is too broad or vague, then the controls will be, by definition, unnecessary regulations that will stifle growth, drive up costs, impede research, curb innovation, and could motivate domestic operations to move overseas. Many of the categories listed in the ANPRM include technologies with existing widespread commercial application and have been freely exportable for years. Any unilateral controls will put the U.S. technology sector at a competitive disadvantage globally and contribute to the rise of foreign technologies and standards developed without U.S. input. The risk of cutting U.S. companies or U.S. persons out of global supply chains and R&D networks through the use of unilateral controls, whether as a result of the letter of the law itself or due to the perception of U.S. companies as potentially unreliable suppliers and R&D partners, is simply too high.

For example, no XX99X ECCNs are controlled at the multilateral level, and placing unilateral controls on these items will cause companies outside the United States to diversify their supply chains away from U.S. suppliers, and potentially exclude U.S. technology from their designs altogether. Indeed, U.S. technology companies have witnessed this phenomenon following recent rulemakings surrounding emerging technology, changes to the foreign direct product rule, and additions to the Entity List.

Countries of concern targeted by unilateral controls that can no longer rely on U.S. technology will advance their own indigenous solutions or replace U.S. components with foreign alternatives. Multinational companies – including those located outside of countries targeted by unilateral controls – will turn to these alternatives rather than using different technology for different regions. Likewise, U.S. companies will lose out on the world’s best scientists and engineers, who will look for work in less restrictive regulatory environments. This shift away from U.S. components and technology serves only to undercut the competitiveness of U.S. companies and undermine U.S. technological leadership, contradicting the sense of Congress in ECRA referenced in the introduction.

As such, ensuring that any proposed controls are agreed to at the multilateral level is imperative to continued U.S. leadership on innovative technologies. We therefore oppose the use of unilateral controls, and only support final controls if the relevant multilateral regime has approved the control or there is a clear path to multilateral agreement.

3 “Ensuring Long-Term U.S. Leadership in Semiconductors,” President’s Council of Advisors on Science and Technology, January 2017.
Potential for Overlapping or Redundant Controls

In testimony presented during legislative consideration of FIRMA, ITI shared its view that “U.S. export control laws and regulations already have the authority to address virtually all, if not all, of the national security risks associated with the contribution or release of ‘emerging critical technologies’ to foreign persons of concern.” While ITI strongly supported the development of “connective tissue” between the Committee on Foreign Investment in the United States (CFIUS) and the export control system, the passage and subsequent ongoing implementation of ECRA have not changed our view regarding the breadth of existing authorities already available through U.S. export control laws and regulations.

As BIS considers whether to apply additional controls to “foundational technologies,” we encourage it to evaluate existing controls and whether such controls already sufficiently meet its desired objectives. Under BIS’s jurisdiction, there is the EAR, the Commerce Control List (CCL), the Entity List, and the Military End Use(r) Rules. The U.S. Department of State administers the International Traffic in Arms Regulations (ITAR) and the U.S. Munitions List as well as U.S. engagement with the Wassenaar Arrangement, Nuclear Suppliers Group, Zangger Committee, Missile Control Technology Regime, and the Australia Group. The U.S. Department of the Treasury manages the Office of Foreign Assets Control (OFAC) Specially Designated Nationals And Blocked Persons List (SDN) and serves as chair for CFIUS. The U.S. Department of Defense (DoD) and the U.S. Department of Energy also have several mechanisms by which to control international transfers of certain items.

Even this cursory overview demonstrates the comprehensive nature of current U.S. export controls regimes, including for the technologies under consideration for the purposes of the ANPRM. For example, the ANPRM notes that “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” and points to China, Russia, and Venezuela as particular countries of concern. It is our view that because many of the items within the categories listed in the ANPRM (i.e., 3A99X, 3B99X, 3E99X, 4A99X, 5A99X, 5D99X) are already controlled under the recently modified military-end use rule (744.21), it is likely that the national security concerns that underpin the ANPRM are already sufficiently addressed and that seeking to control additional items in these categories will only result in over-controlling. At a minimum, BIS should carefully analyze the impact of newer restrictions recently imposed on Russia, Venezuela, China, and various Chinese companies before imposing any new restrictions on “foundational technologies” to serve the same purpose as these existing restrictions.

The scope of what could be considered as foundational technologies is grounded in the characteristics identified in ECRA. However, the ANPRM also makes clear that items currently controlled for reasons such as anti-terrorism (AT), crime control (CC) or short supply (SS); subject to United Nations embargoes; or designated as EAR99 are under consideration to be identified as foundational technologies. This inherently raises concern about a scenario in which an item could be simultaneously controlled under multiple U.S. export control regimes and underscores the point that the technologies under consideration are already subject to existing U.S. export control regimes.

---

4 H.R. 4311, the Foreign Investment Risk Review Modernization Act of 2017: Hearing before the Subcommittee on Monetary Policy and Trade of the House Committee on Financial Services, April 12, 2018 (testimony of Jonathan (Josh) S. Kallmer),
Additionally, while it is somewhat unclear whether items controlled for CC purposes are in scope for consideration under this ANPRM,\(^5\) we ask that BIS exclude CC-controlled items from this exercise given they are already being addressed in another simultaneous rulemaking under review, to which ITI has also submitted a response.\(^6\)

**Implications for CFIUS**

The U.S. Department of the Treasury released in September 2020 a final rule for the treatment of certain transactions involving critical technologies, pursuant to reforms made through FIRRMA. Any foundational technology identified through this interagency process led by BIS would – in combination with other factors – trigger a mandatory filing to CFIUS under existing rules as well as the final rule. ITI encourages BIS to closely consult with CFIUS colleagues at the U.S. Department of the Treasury and other participating agencies to understand how the identification of foundational technologies may impact the number of transactions that would require mandatory filings and potentially impact CFIUS’s ability to evaluate transactions in a timely, predictable, and thorough manner. Maintaining the United States’ status as a top destination for foreign R&D investment is a critical component of strengthening U.S. technological and economic leadership.

**Keeping the Focus on ECRA’s Mandate**

Lastly, we respectfully request export controls not be deployed as a tool to advance trade policy, industrial policy, or trade protectionism. ECRA’s mandate does not extend to these areas, which are better addressed through other provisions of law relevant to those topics. Export controls should be used exclusively to address true national security concerns.

**Scoping Ideas**

Congress established through ECRA clear statutory standards for the conditions under which technologies could be controlled as “foundational.” For example, ECRA section 4817(a)(1)(B) outlines that BIS must consider “the development of emerging and foundational technologies in foreign countries; the effect export controls imposed pursuant to this section may have on the development of such technologies in the United States; and the effectiveness of export controls imposed pursuant to this section on limiting the proliferation of emerging and foundational technologies to foreign countries.” Based on these considerations, ITI believes that any ensuing controls of foundational technologies be limited to those technologies that only exist in the United States. The majority of foundational technologies have global availability, are taught at universities, are manufactured in different places around the world, or have matured to a publicly available or obtainable technology.

ITI finds particularly concerning BIS’s stipulation in the ANPRM that “the term foundational technologies includes not only ‘technology’ but also ‘commodities’ and ‘software’ as used in the EAR.” There is no authority under ECRA section 4817 – which provides the statutory standard for scoping new controls for emerging and foundational technologies – to regulate commodities or

---

\(^5\) The “Background” section of the ANPRM identifies that CC-controlled items are amongst those subject to the EAR but not covered by the DPA’s definition of “critical technologies,” but CC-controlled items are not amongst those identified in the categories described in the ANPRM’s third question.

software. While BIS has the authority to administer controls for commodities and software through the EAR and other aspects of ECRA, ITI urges BIS to limit its consideration of “foundational technologies” to technologies as reflected in section 4817 for the purposes of this particular rulemaking.

Proposed Definition for “Foundational Technologies”

ITI proposes the following definition for “foundational technologies,” which is drawn from statements of policy in ECRA and the Federal Register Notice for the ANPRM.

“Foundational technologies” are specific core “technologies” that the Bureau of Industry and Security has determined to be:

(a) unavailable in or not otherwise being developed in foreign countries;

(b) not within the scope of any existing multilateral controls;

(c) essential to the national security interests of the United States; and

(d) “required” for the “development,” “production,” “use,” operation, installation, maintenance, repair, overhaul, or refurbishing of items that are:

(i) conventional weapons, for intelligence collection applications, weapons of mass destruction, or terrorist applications; or

(ii) could support illicit procurement attempts which may demonstrate some level of dependency on U.S. technologies to further foreign military or intelligence capabilities in countries of concern or development of weapons of mass destruction.

Note 1: A “technology” must not be identified or controlled as “foundational” unless it is within the scope of policy statements in ECRA. In particular, a “technology” must not be identified as “foundational” if a unilateral export control over it would:

(a) significantly harm domestic research on the identified “technology;”

(b) be ineffective at preventing countries of concern from developing it indigenously or otherwise acquiring comparable “technology” from third countries;

(c) be imposed without a full consideration of the impact on the United States’ economy of such a control; or
(d) be of a type that is not likely to be considered acceptable by the multilateral regime allies or that is inconsistent with the standards for the types of controls that are subject to the multilateral regimes.

Note 2: This definition does not apply to an exporter’s determination of whether a “technology” is “foundational.” Rather, it governs BIS determinations regarding whether a specific “technology” should be added to the Commerce Control List as a “foundational technology.”

As noted above, each of the elements in the proposed definition is taken from the requirements in ECRA and BIS’s notice. It also uses as many of the existing EAR definitions and concepts as possible to avoid confusion in its application. In addition, the proposed definition reinforces the core policy element of ECRA that unilateral controls are disfavored. This places on BIS the burden of demonstrating that each of the statutory requirements for the imposition of such controls has been met. The definition also reflects logical and factual points, as discussed below, that the U.S. Government, rather than industry, should identify what the national security threat is that needs to be addressed through the use of unilateral controls.

However, if, as stated in the notice, BIS intends to apply the identification and control effort to “items,” not just “technologies,” then our suggestion for a definition (for the same reasons) would be:

“Foundational items” are specific core “items” that the Bureau of Industry and Security has determined to be:

(a) unavailable in or not otherwise being developed in foreign countries;

(b) not within the scope of any existing multilateral controls;

(c) essential to the national security interests of the United States; and

(d) necessary for any of the following items, applications, or efforts:

(i) conventional weapons, intelligence collection applications, weapons of mass destruction, or terrorist applications; or

(ii) could support illicit procurement attempts that may demonstrate some level of dependency on the items to further foreign military or intelligence capabilities in countries of concern or development of weapons of mass destruction.

Note 1: An “item” must not be identified or controlled as “foundational” unless it is within the scope of requirements in ECRA section 4817. In particular, such
items must not be identified as “foundational” if a unilateral export control over it would:

(a) significantly harm domestic research on the identified “item;”

(b) be ineffective at preventing countries of concern from developing it indigenously or otherwise acquiring comparable “items” from third countries;

(c) be imposed without a full consideration of the impact on the United States’ economy of such a control; or

(d) be of a type that is not likely to be considered acceptable by the multilateral regime allies or that is inconsistent with the requirements for the types of controls that are subject to the multilateral regimes.

Note 2: This definition does not apply to an exporter’s determination of whether a “item” is “foundational.” Rather, it governs BIS determinations regarding whether a specific “item” should be added to the Commerce Control List as a “foundational item.”

Answers to Specific Questions
ITI welcomes the opportunity to respond to specific questions posed by BIS.

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

We point BIS to the above scoping comments, which include a proposed way by which to define foundational technology.

2) Sources to identify such items;

Absent additional guidance from BIS on which technologies or items it considers to be “foundational” beyond the categories listed in the ANPRM, it is difficult for us to identify specific items that may be of concern. As a general matter, we believe that because many of the items in the categories set forth in the ANPRM have been freely exportable for years and are now globally ubiquitous, there is little to no national security risk in maintaining the status quo. Upsetting the status quo would likely stifle U.S. companies’ ability to innovate, while allowing other companies that do not contribute to U.S. technological leadership to grow.
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;**

We believe that the U.S. Government is better positioned than industry to determine which items or technologies are essential to U.S. national security and/or provide a quantifiable military advantage. However, we reiterate that many technologies that fall under the categories listed in the ANPRM (i.e., consumer and enterprise computing hardware and other consumer electronics classified as 5A992, 3A991, or 3A992) are already globally ubiquitous and thus, new unilateral export controls will not limit the proliferation of these items worldwide. They would instead lead companies outside of the United States – and not just in countries of concern – to develop and use non-U.S. products and services, thereby negatively impacting the U.S. economy. They would lead companies in countries of concern to develop indigenous and potentially globally competitive alternatives.

At a minimum, BIS should issue a notice of proposed rulemaking and solicit public comments on any contemplated additional regulation of items. Per the definition above, the notice of proposed rulemaking should specify, to the maximum extent possible in a public document, the specific weapon, military, or intelligence application to which the item is essential, and should identify the parameters and outcomes of the foreign availability study undertaken by BIS to conclude that the item is not already produced or available outside the United States.

4) **The status of development of foundational technologies in the United States and other countries;**

There are several existing U.S. resources that may provide information about the status of development of technologies:

- The U.S. Patent and Trademark Office (PTO), which is part of the Commerce Department and already has a procedure and mandate to prevent publication of certain types of sensitive patent applications.
- The National Institute of Standards and Technology (NIST), which is also part of the Commerce Department.
- The BIS Technical Advisory Committees.
- The Small Business Innovation Research (SBIR) Program.
- The Small Business Technology Transfer (STTR) Program.
- International standards development bodies, such as ISO, IEC, or IEEE.
- All DoD-funded research labs, such as the Defense Advanced Research Projects Agency (DARPA).
- Reports from market research firms such as Gartner.
- Interviews with venture capitalist and entrepreneur seed money investment groups.

Other resources include international standards bodies. If an standards development organization is working on technology-specific standards, then by its nature that technology would already be internationally available. Companies may be able to submit information regarding foreign
availability of certain technologies, although they may be better positioned to speak to whether there are competitors ready to absorb their market share and not necessarily their competitors’ state of development.

Additionally, licensing exports is one of the most effective ways Commerce can grasp which U.S. technologies and capabilities are available overseas. As such, it is critical to consider how the presumption of denial (whether perceived or otherwise) may have unintended consequences. If firms assume that their license applications will be rejected, they will be less likely to submit them. That would not only stymie the optimization of R&D operations, it would cut off American technology from global supply chains and the Commerce Department would lose a vital source of information on where technologies are flowing.

Regulating foundational technology presents a unique challenge that was not present in BIS’s efforts to identify and place appropriate controls on “emerging technology.” Almost by definition, foundational technologies are so well-established as to be globally ubiquitous, such that even multilateral export controls will not meaningfully limit the availability or use of these technologies outside of the countries that impose such controls.

**Mass-Market Encryption**
Of the categories listed in the ANPRM, one example to carefully consider is mass-market encryption items classified under ECCNs 5A992 and 5D992. Based on conclusions BIS reached in decontrolling certain encryption items in 2010, additional controls on these mass-market items will serve to diminish U.S. national security by making U.S. encryption products less competitive across the globe. More specifically, 5X992 items are subject to the recently expanded military end-use/user controls in Supplement 2 to Section 744.21 of the EAR, and the ANPRM specifically identifies technologies identified in this supplement as potential candidates for additional “foundational technology” controls.

Much of the hardware and software that provide 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) are classified under these “mass-market” encryption categories. Imposing additional export 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 do not want to rely on technology they can use in, for example, Europe, but not in China or Russia. That gap will then be filled by companies that are not headquartered or otherwise do not have presence in the United States, potentially even by companies from the very countries the controls target. This will harm U.S. companies and U.S. national security by diminishing the overall use and influence of American products and companies abroad. Indeed, such an action would provide an economic and diplomatic boost to companies, like Huawei, who are well-positioned to saturate these markets, even with inferior technology, if U.S. suppliers are suddenly unable to sell their products. This may also diminish national security through a schism in global encryption standards wherein more products will gravitate towards

---

proprietary encryption standards developed by foreign governments rather than globally accepted standards like AES-128.

Additionally, mass-market status is premised in part on the ubiquity of this technology – i.e., one criteria to qualify for a 5X992 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 in part to correct initially overly broad encryption controls and to “enhance national security by ensuring the continued competitiveness of U.S. encryption products.” This rationale continues to apply, and 5X992 items that were recently decontrolled to enhance national security should not now be subject to new, ineffective controls.

**Microprocessor Hardware and Technology**

Design of category 3 semiconductor technology, one of the categories listed in the ANPRM, takes place all over the world, including in the United States, Taiwan, the United Kingdom, China, South Korea, and Israel. U.S. semiconductor companies also work with design teams throughout the world. Further, global companies, including at least one Chinese company, Alibaba, are already using the RISC-V “free and open” standardized instruction set architecture (https://riscv.org/about/) to develop high-performing microprocessors. In light of these design and development activities, additional controls on exports of microprocessors and microprocessor design technology would be ineffective because microprocessor design activity is already dispersed globally, and limiting the ability of U.S. companies to export microprocessors and microprocessor designs could provide a competitive advantage to non-U.S. companies in this industry.

Some of the world’s foremost semiconductor manufacturers are located outside the U.S. BIS has already taken steps, through the expansion of the foreign direct product rule and other restrictions on dealing with Huawei, HiSilicon, and other Chinese companies of concern, to cut off these companies’ access to U.S. technology and to manufacturing facilities that employ U.S. technology.

Given these current restrictions, it is highly unlikely that additional restrictions in the form of unilateral export controls on 3A991/2 hardware or 3E991 technology would yield any new security advantage.

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

Deemed export requirements, in particular, would greatly harm the continued development of “foundational technologies” in the United States. We strongly recommend against any deemed export or deemed reexport controls on categories listed in the ANPRM and encourage BIS to

______________________________

8 Id.
9 Id at 36483.
consider whether companies’ own security and intellectual property-focused protections would supplant or exceed any benefits that could be gained through deemed export requirements.

Although the United States has traditionally been the leader in many technologies covered by the categories listed in the ANPRM, these technologies are now globally ubiquitous and other countries are steadily developing and producing these technologies alongside the United States, driving competition and innovation. To stay competitive in the development and implementation of these technologies, U.S. companies, think tanks, universities, and research organizations require access to the most talented scientists and engineers, regardless of location or nationality. These talented individuals want to work and collaborate with the best scientists and engineers from around the world in the least restrictive regulatory environment. Unilaterally controlling the export of any technologies in the categories listed in the ANPRM would restrict only U.S. companies’ access to this global talent, while foreign companies would be able to attract the best talent and leverage foreign contributions without being subject to these restrictions. This would damage the ability of U.S. industry to compete in an open global marketplace for the best people, undermine U.S. technological leadership, and negatively impact the U.S. economy.

More generally, broad and overly burdensome controls restricting U.S. companies from full participation in the vibrant global exchange of technologies would undermine U.S. technological leadership even beyond any items identified as “foundational technologies.” Other countries’ technologies would inform global standards and seek adoption in global products and services. U.S. companies would lose both the ability to influence these standards as well as access to global export markets for their products and services. Innovators or startups developing the next generation of “foundational technology” would elect to develop somewhere outside the United States free of these restrictions, taking high-quality U.S. jobs with them. To ensure that export controls do not block U.S. economic and technological growth and leadership, BIS should consider whether existing export controls, including list-based controls such as the BIS Entity List and OFAC’s SDN list, satisfy the national security goals of any contemplated regulations on “foundational technology,” and, at most, should only impose narrowly tailored controls that are agreed at a multilateral level, are demonstrably essential to U.S. national security interests (per the definition proposed above), and provide exemptions that allow these technologies to continue to move freely amongst U.S. companies, their non-U.S. subsidiaries, and the employees of these companies inside and outside the United States.

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

BIS should not impose new end-use/user restrictions on specific “foundational technologies” absent specific, list-based designations which identify specific entities of concern.

As we reference above in our section on Potential for Overlapping or Redundant Controls on page 6, the ANPRM explicitly notes that many of the items within the categories listed (e.g., 3A99X, 3B99X, 3E99X 4A99X, 5A99X, 5D99X) are already controlled for export in support of military end-uses/users in sensitive countries, which would seem to address one of the key concerns mentioned in the ANPRM, that “many items can be tied to indigenous military innovation efforts in China, Russia or Venezuela...[and] may pose a national security threat.”
We also caution BIS that in some cases where a license has been triggered for military end-use/user reasons, the situation may be specific to that end-user and therefore, application of or use of the technologies is not widely concerning in other parts of the country. Hence, a broad, list-based control based on country will be unhelpful in addressing legitimate national security concerns. To the extent BIS is interested in adding additional controls to the categories listed to address national security concerns, it should do so not by imposing broad controls on entire categories of ubiquitous technologies, but instead by updating the Entity List, where appropriate, to reflect any changes to military end-uses or end users.

Most companies that trade in items in the categories listed in the ANPRM (as well as other technological items subject to the EAR) have sophisticated screening systems to monitor companies’ customer bases against changes to, e.g., the BIS Entity List or OFAC’s SDN list, although opaque ownership structures and the complexity of systematically and at scale discerning authorized from unauthorized activity can sometimes pose challenges for such screening approaches. In addition, end-use restrictions may be useful for addressing nefarious uses of greatest concern; however, nefarious end uses can be difficult to detect at scale and are therefore ineffective where U.S. exporters often rely on attestations from the very entities carrying out these uses.

Broad end-use restrictions that are not specific to entities present huge compliance challenges to U.S. industry and can be difficult to scale. Although U.S. exporters undertake their best efforts with respect to “know your customer” (KYC) due diligence on customers, this work creates a tremendous amount of compliance overhead and is ultimately not an effective mechanism for determining whether one customer out of hundreds, thousands, or tens of thousands may intend to use U.S. technology for a nefarious purpose. In almost all instances, the U.S. government has more and better information than private industry about whether a particular entity presents a threat to national security, and the government can effectively manage that threat by identifying such entities as SDNs or on the BIS Entity List.

If Commerce decides to pursue end-use/user controls in some capacity, we suggest that in order to address the aforementioned challenges Commerce explore the potential for use of novel technological solutions to more nimbly implement end-use and end-user controls 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.

In addition to the list-based controls discussed above, existing technology-based controls and in-progress processes for updating these controls are sufficient.

Finally, we recommend that BIS consider making public the results of its determinations with regard to military end-users based on licensing applications submitted under 744.21. It does not make sense that only the company that submitted the license application should know whether a company has been designated a military end-user. Indeed, all exporters should have access to this information regarding articulable national security interests so that neither they nor BIS have to reinvent the wheel each time they plan to export. It seems unhelpful to have companies performing the same resource-intensive due diligence on the same companies every time they want to export if BIS has this information and is able to provide it in a public fashion. This will also help to ensure a level economic playing field and ensure that national security concerns are addressed in a consistent way.

Promoting Innovation Worldwide

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

No enabling technologies, including but not limited to tooling, testing, and certification equipment, should be included within the scope of a foundational technology. Testing technologies are used for measuring to an international standard, and this type of equipment is made in many other countries across the globe and as such should not be included. Enabling technologies are used for testing the general function, safety, circuitry, performance, tuning, or repairing of an item. Many companies will use these technologies in design or production facilities, or license them to contract manufacturers or other partners to ensure quality of production. However, without knowing how the technology under evaluation works, the enabling or testing technologies will not be helpful. Further, mass production, testing, and cost will suffer if they are required to stay in the United States.

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.

As a general matter and based on our arguments above, it is our view that unless any new controls meet the rigorous thresholds established in ECRA and outlined in our comment, new restrictions on technologies based on their “foundational” status are unnecessary and will be ineffective in limiting the global development and proliferation of these already-ubiquitous technologies. If any new restrictions are required for national security reasons, BIS and/or OFAC should use their existing authorities to designate entities that threaten U.S. national security under the BIS Entity List or as SDNs. BIS should consider novel technological solutions to more effectively administer these restrictions. Furthermore, if BIS, contrary to the economic interests of thousands of U.S. companies and tens of thousands of U.S. workers, opts to place additional restrictions on specific technologies, BIS should – at a minimum – ensure that there are license exemptions so that these technologies can continue to move freely between and amongst U.S. companies, their overseas subsidiaries, and foreign national employees in the U.S. and abroad. Any changes should also include a sufficient grace period for companies to make necessary adjustments to comply.

Conclusion
Thank you for providing an opportunity for our member companies to comment on the ANPRM. As our letter demonstrates, the breadth of rulemaking to implement section 1758 of ECRA is of critical concern to our member companies. Any efforts to strengthen controls for reasons of U.S. national security must be narrowly tailored to specific and essential national security threats so as not to inadvertently harm U.S. companies’ global technology leadership or detract from the United States’ attractiveness as a top destination for international R&D spending, which are in and of themselves essential to realizing the short- and long-term national security objectives of the United States. We appreciate BIS’s consideration of our perspectives and look forward to continuing to work with the U.S. Department of Commerce, interagency colleagues, and other stakeholders as you develop these regulations.