January 10, 2019

Honorable Richard Ashooh
U.S. Assistant Secretary of Commerce for Export Administration
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
1401 Constitution Ave, NW
Washington, DC 20230

Subject: Comment on ANPRM Regarding Review of Controls for Certain Emerging Technologies

Reference: 83 Fed. Reg. 58201; RIN 0694-AH61; Docket # 180712626-8840-01

Dear Mr. Assistant Secretary:

The Information Technology Industry Council (ITI) represents the global voice of the high-tech community, 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 60 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. Most of our members are headquartered or significantly invested in the United States, and their investments have not only propelled economic growth and innovation across the U.S., but they have also launched new industries and advanced new markets around the world.

ITI appreciates the opportunity to provide comments in response to the Advance Notice of Proposed Rulemaking (ANPRM) regarding the Review of Controls for Certain Emerging Technologies. We feel compelled to note at the outset the limitations created by the relatively short timeframe for response, the highly complicated technological areas identified in the ANPRM, and the lack of a confidential feedback channel. BIS's request for information implicates complex policy and technological concerns. Preparing comprehensive comments in less than 60 days has presented a challenge for ITI and its members. We understand and appreciate BIS's intent to provide the opportunity to comment on the proposed rules before any interim or final controls are imposed, as well as BIS's intent to launch a separate process to examine foundational technologies. We would urge BIS to provide additional time for these next steps with a minimum of at least 90 days for comments. Additionally, given that some of the information BIS is soliciting in the ANPRM is

Global Headquarters
1101 K Street NW, Suite 610
Washington, D.C. 20005, USA
+1 202-737-8888

Europe Office
168 Avenue de Cortenbergh
1000 Brussels, Belgium
0032 (0)2 380 7764

info@itic.org
itic.org

sensitive, we urge BIS to develop a process that safeguards information provided by industry participants to avoid the disclosure of business proprietary or confidential information.

Principles for Emerging Technology Export Controls

We recognize that concerns about U.S. national security are at the heart of this ANPRM. American companies have long spearheaded the most innovative and cutting-edge technologies, transforming the global economy and catalyzing tremendous growth for 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 science and technology fields. In recent years, there has been great emphasis on China in this regard.

ITI and its member companies support the national security goals of the U.S. government. At the same time, 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.

The breadth and the number of technologies in the ANPRM suggest that BIS is considering a potentially significant expansion of the U.S. export control regime. Before responding to the questions presented in the ANPRM, we share some key principles to guide the Administration's approach to new export control requirements on emerging technologies:

- The export control regime should be used to advance and protect U.S. national security interests without risking American competitiveness in emerging technologies.
- The scope of new emerging controls, by statute, should be limited to those that are "essential" to the national security of the United States.
- The scope of new emerging controls, by stated policy objectives, should be limited to those that provide a specific identifiable and qualitative military advantage.
- Export controls should be placed on the use of technologies (not the technologies themselves, as many of the technological categories have been in production in the market).
- Export controls should not be placed on long-established technologies that are available outside the United States, or on published technology and information sources, even if they are among those listed in the ANPRM as potential "emerging" technologies.
- Technologies that are currently controlled under existing export controls should not be considered for controls as "emerging" technologies.
- If unilateral designations and controls are contemplated, special consideration should be given to the impact of any licensing policy on U.S. businesses and their role in researching and

developing technologies, as well as supporting American leadership and international competitiveness.

- Identified technologies that meet the statutory standards 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.

- Additionally, final rules establishing unilateral export controls on any item should not be published until the relevant multilateral regime has approved the control or has a clear path to agreement.

- Export controls should not be used as a lever in trade policy.

- BIS should look to past U.S. best practices when contemplating its expansion of the export control regime.

- Existing license exceptions, exclusions, or authorizations should apply to any controls on "emerging" technologies.

- BIS should create license exceptions, or other mechanisms, to allow for vital intra-company exports, re-exports, and transfers between and amongst: U.S. companies and subsidiaries; their non-U.S. counterparts; and intra-company deemed exports to foreign nationals.

National security objectives should be defined

ITI members are committed to working with the U.S. government to support critical national security objectives. An essential first step is mutual understanding of how industry can effectively help the government reach these objectives. A threshold question that we need the U.S. government to answer is: where are the gaps between existing controls over technology and the current and emerging threats? We believe it is essential for the government to clearly identify and communicate the linkage between emerging technologies and threats so that industry can provide its expertise regarding these technologies. We respectfully ask the Administration to define clearly in any proposed rule national security threats that are not currently being addressed by existing controls. With such clear communication as a foundation, we believe government and industry can more effectively work to identify specific technology applications that address clearly articulated national security concerns.

New export controls should be tailored to meet essential national security objectives

To the goal of identifying those technology controls "essential" to national security, we note that the notice goes beyond that standard by asking for advice about technologies that are "important" to the national security of the United States. ECRA Section 1758 limits the scope of new emerging controls to those that are "essential" to the national security of the United States. Controls should not be imposed on technologies that are merely used or usable by the U.S. military. For a thorough and informed strategy, the Administration should define the term "essential", particularly given that the defense sector is increasingly dependent on commercial-off-the-shelf dual-use technology. An overly expansive approach that controls technologies that do not meet the "essential" standard will handicap U.S. companies from staying ahead of their competition, which will ultimately serve to

undermine – not support – U.S. national security. Because ECRA states that unilateral controls should be limited, a higher standard – the "essential" standard – is required in this effort. We urge BIS to work with industry to hone in on those uses without capturing entire categories of widely-used technologies. Further, the scope of new controls, according to the stated policy objectives of this ANPRM, should be limited to those that provide a specific identifiable and qualitative military advantage.

BIS should focus on use of technologies

In addition, we think it is important to distinguish between the broad categories of technologies as listed in the ANPRM and the specific use of those technologies for the purposes of establishing appropriate export controls. We would submit that rather than the basic technology being of national security concern, it is the specific use. For instance, cybersecurity technologies can be used for defensive and preventive purposes to protect organizations in all industry sectors from successful cyberattacks. Given the interconnected nature of the global digital infrastructure, controlling cybersecurity technology could have unintended and counterproductive consequences, such as slowing the discovery and disclosure of critical vulnerabilities to U.S. internet infrastructure. We believe this distinction to be essential and foundational to BIS's work on identifying emerging technologies' impact on national security.

Controls should not be placed on established technologies

Relatedly, it has been long established in the U.S. export control regime and reiterated in ECRA itself that certain technologies – those that have been around for decades and are publicly available including outside the United States – are not subject to export controls. Retroactively controlling these technologies, even if they are among the ANPRM categories or used in or to develop technologies in these categories, would prove to be complex, ineffective, and inconsistent with the aims of the ANPRM. Any attempt to impose controls in these circumstances will create opportunities for these established technologies to be further developed and used outside the U.S., while creating no national security benefit for the U.S. For example, there are a number of technology categories included on the ANPRM list, such as AI evolution and genetic algorithms, experts systems research, and logistics modeling and optimization technology, which have been used to solve mathematical optimization problems for over thirty years and on which there are large bodies of literature and research, in the U.S. and globally. For example, much of the current AI enabling technology is available under licenses that have largely put the "tools" in the hands of global researchers and implementers. For example, tool kits are freely distributed, consumed and modified by companies and individuals globally. These tools are becoming standard in training machine learning algorithms and, as such, speak to the base technology itself.

We are concerned that an expanded export control regime, based on new criteria but untethered from "uses" tied to essential security concerns, could create unnecessary burdens on our member companies to which other foreign competitors would not be subject. Depending on the scope of the controls, any number of elements of a product or exchange of know-how may require an export control license. For example, product software, hardware, and research partnerships with foreign companies may all require licenses in technology areas that today are commonly being researched at non-U.S. companies and institutions. An overly-broad list of "emerging" technologies could cause

significant delays and hurdles that could prevent a company from conducting business that would not damage U.S. national security. Foreign companies that will not have to contend with such requirements and potential impediments are likely to gain economic and technological advantages. Further, broad controls could also undermine the business models of many companies that have adopted distributive network architectures that rely on the ability to deploy software and other technologies in local markets around the world.

Limit controls to technologies that are only available in the U.S.

Further, we urge BIS to look to limit controls to those technologies/ adoptions of technologies that are only developed and available in the United States. The effort to develop cutting edge commercial uses of technologies is truly global in nature. U.S. semiconductor companies, for example, must work with hardware companies years in advance of system deployment in order to win business and ensure integration of U.S. products in those systems (i.e., 5G). Overly expansive controls could result in the "designing out" of American-made components to the advantage of foreign companies with comparable products that are not subject to similar controls. That would have a further degrading national security effect of creating vulnerabilities for foreign influence, access, or control over critical products or services in the U.S. Identifying those areas where U.S. technology is truly ahead of the curve and developed exclusively in the U.S. is critical to address national security implications of emerging technologies.

Avoid imposing unilateral controls

Relatedly, avoiding unilateral controls is imperative to ensuring U.S. leadership on innovative technologies. In cases where there is global competition, a unilateral control causes direct harm to U.S. companies. 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, and motivate domestic operations to move overseas. Many of the representative technology categories listed in the ANPRM are those with existing widespread commercial application. Long-term unilateral controls will harm the U.S. tech sector's ability to compete globally. As such, the establishment of multi-lateral controls is imperative to ensure U.S. leadership on innovative technologies. We therefore oppose the use of unilateral controls, and only support controls if there is a clear path to agreement by all Wassenaar member countries.

Resist deploying export controls as a trade policy tool

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 other areas which are better addressed through other provisions of law relevant to those topics.

Look to past U.S. best practices

In addressing the complex challenge of exploring controls over emerging technologies to protect national security, ITI urges BIS to take stock of best practices that have worked in the past, such as cryptography. Humans have been applying cryptography for thousands of years. During the Second World War, encryption – a technological application of cryptography that enabled secure military communications – was "critical" to enable U.S. victory. While Germany and Japan also had encryption applications, the technology the U.S. was using was unique. The U.S. export control

regime banned the sale of certain types of strong encryption software essential to national security, and these technologies were classified as "munitions" under U.S. law, alongside semiautomatic weapons and nuclear warheads. As digital and telecommunications capabilities evolved and encryption software became globally available and essential to the communication and transmission of sensitive commercial data, the national security value of export controls eroded and the controls began having an adverse impact on U.S. businesses, limiting their sales and the growth of e-commerce. Eventually, in 1996, President Clinton signed an executive order to loosen those restrictions. Today, encryption products are considered standard components of major sales features for American and foreign companies.

Existing license exceptions should apply to any controls and new export controls must allow for intra-company transfers

Existing license exceptions, exclusions, or authorizations should apply to any controls on "emerging" technologies. In addition, BIS must use license exceptions or other mechanisms to allow for unrestricted intra-company exports, re-exports, and transfers between and amongst U.S. companies and subsidiaries and their non-U.S. counterparts. BIS should also provide an exception for intra-company deemed exports to foreign national employees of the U.S. operation and its non-U.S. subsidiaries. This will help to ensure that access to ideas and technologies within multinational U.S. companies will be preserved, allowing these companies to continue innovation and technological leadership.

ANPRM Questions

How to define emerging technology to assist identification of such technology in the future?

The first question posed is critical—how should BIS define emerging technology for the purposes of this rule-making? To meaningfully scope a definition, it is essential to understand the underlying policy objectives. Thus, we suggest that the definition of "emerging technologies" be structured around and bounded by the statements of policy in ECRA.

ITI's proposed definition of "emerging technologies[1]" is the following:

"Emerging technologies" are specific technologies that:

(a) are "required" for the "development" of items that:

(i) are essential to the national security interests of the United States;

(ii) provide the United States with a specific and identifiable qualitative military advantage; and

[1] This definition is based on existing terminology in the Export Administration Regulations ("EAR") from 15 C.F.R. § 772. These terms are widely understood and applied by the corporate and academic communities.

(iii) are not identified on the Commerce Control List or the United States Munitions List; and

(b) are not available in or being produced in foreign countries; and

(c) do not include "production" technology or any aspect of "use" technology for items in production.

To further elaborate, as BIS considers the key threshold definition of "emerging technologies," we recommend that BIS look to the helpful guidance provided in ECRA, including policy statements that can effectively serve as guardrails for defining which technologies must not be identified or controlled as "emerging." Specifically, ECRA's guidance provides that a technology must not be so identified if a unilateral export control over it would:

(i) harm domestic research into the identified technology;

(ii) not be effective at preventing countries of concern from developing it indigenously or otherwise acquiring comparable technology from third countries;

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

(iv) is 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.

Criteria to apply to determine whether there are specific technologies within these general categories that are important to U.S. national security?

- *Would the identified technology provide a qualitative, tangible advantage to the U.S. defense sector for a significant period of time?*
- *Is the technology in high value production and already available in other countries?*
- *Has a patent been filed?*
- *Would technology controls hinder the development or commercialization of the U.S. technology?*
- *Would technology controls result in U.S. technology being designed-out of products developed by other nations, including friendly nations?*
- *Would technology controls lead target nations to launch initiatives that could ultimately harm U.S. companies by creating competitors?*
- *Would the controls duplicate end-use (proliferation) controls in Part 744?*
- *Are technology controls the best and most appropriate means to address the overall threat, or is there a better, "run faster" strategy to comprehensively address the full scope of the threat, including, for example, direct investment?*

Sources to identify such 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.
- Standards bodies, such as ISO, IEEE, or 3GPP.
- 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.

ECRA Section 1793 mandates the Secretary of Defense and Director of National Intelligence to submit a report to Congress on "certain defense technologies critical to the United States maintaining superior military capabilities. This report will, among other things, identify "key areas in which the United States currently enjoys a technological advantage" as well as "key areas in which the United States no longer enjoys a technological advantage". BIS should take this report into account when identifying emerging technologies on which to establish controls, and in particular avoid controls on technologies that fall into the latter category. While outside the scope of these comments, ITI is interested in the standards that will be used to determine whether the United States has, or does not have, the leading edge or advantage in a given area of technology.

The status of development of these technologies in the United States and other countries?

A number of the technologies listed are the subject of intense global competition among companies, universities, governments/nation states, and other research entities. All the types of technology our members are engaged on are also the subject of research and product deployment by other entities outside the U.S., as described in greater detail below. As such, restricting the export of these technologies will not prevent foreign entities from obtaining them. Rather, it will only prevent them from obtaining U.S.-developed versions and thus harm U.S.-based companies and American workers.

We note that the Secretary of Commerce is required under Section 1754(a)(6) to "establish a process for an assessment to determine whether a foreign item is comparable in quality to an item controlled under this part, and is available in sufficient quantities to render the United States export control of that item or the denial of a license ineffective, including a mechanism to address that disparity". We believe the question of foreign availability is fundamental to whether or not BIS should establish a control upon an identified "emerging technology". We ask BIS to articulate what process it has in place, or is developing, to make the foreign availability assessment required by the ECRA. Especially given the rapid pace of development that is occurring in many of the ANPRM technology fields, BIS must create a process that will enable industry to quickly and easily bring evidence of parallel development and production activity involving any controlled emerging technologies outside of the

United States so that BIS can act to modify its controls in ways to ensure that U.S. companies can remain competitive.

The impact specific technology controls would have on U.S. technological leadership?

Overbroad export controls and licensing requirements would have a fundamental impact on U.S. technological leadership, impeding the ability to attract talent and participate in the global research efforts, and ultimately impacting the successful launch of products and services. Excessive controls can have the adverse impact of hindering U.S. technological competitiveness and innovation to the advantage of foreign entities. Foreign companies that do not have to contend with as many compliance and licensing restrictions will gain an inherent advantage. In order for U.S. industry to continue to be the most innovative in the world – in fields that may have national security relevance – they must be able to compete, attract investment and talented workers, and learn from and outpace competitors. This type of competitive advantage cannot be developed in a vacuum, and excessive controls may have negative and unintended consequences for both longer-term competitiveness and security.

Another critical consideration of expanded export controls is the ability of U.S. technology companies to attract and retain talent. Competition for an educated, skilled labor force based on U.S. and non-U.S. talent in the technology sector is fierce. At the same time, the United States faces a shortage of science, technology, engineering, and mathematics (STEM) workers, and the U.S education system is not producing a sufficient number of graduates with STEM degrees. According to a 2014 report from the Brookings Institution, STEM positions take longer to fill than openings in other fields. Additionally, as found in a 2013 report from the Information Technology and Innovation Foundation, U.S. technology companies often rely on foreign talent to "fuel the U.S. innovation economy that the United States cannot provide on its own."

Companies seek to hire highly-qualified graduates from U.S. and non-U.S. universities. If non-U.S. talent is not hired by U.S. companies, these highly in-demand individuals are likely to return home. American technological competitiveness therefore requires that U.S. companies attract and retain the best and the brightest, irrespective of nationality. However, this challenge of recruiting and retaining top talent is one that U.S. technology companies are already facing in the competitive global marketplace. Overly strict licensing requirements, long delays for the issuance of licenses, or perceived challenging of obtaining licenses that further limit the ability of U.S. employers to hire the best and brightest from outside the U.S. could cause such individuals to take their talents elsewhere.

Process Considerations

Our members have also shared a number of comments regarding the process to develop ECRA implementing regulations. First, as stated in our introduction, the condensed timeline for these comments has created challenges for all of our members. The breadth of scope of technologies under consideration combined with the complex and sensitive nature of the subject matter requires deep and broad engagement across multiple lines of business. Additional time would have certainly afforded a deeper dive. We hope to have 90 days for the next stages of BIS's rulemaking on emerging technologies and request a longer comment period for the forthcoming notice on foundational

technologies. ITI strongly encourages BIS to establish a confidential channel of communication with the business community to solicit additional information. A process that requires sensitive and proprietary business information to be shared publicly will come up short. We recommend an established confidential channel to ensure businesses have a way to offer feedback without risk of disclosure.

ITI member engagement does not end with the final rule/s on ECRA. We recommend BIS include in its rulemaking clear and transparent processes concerning the review of controls on emerging technologies. Specifically, we recommend that BIS elaborate not just on the process for adding technologies to the list but also removing or modifying them. 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 how rapid technological advancement can be, this point is especially critical to this regulation. We also recommend BIS establish a mechanism by which stakeholders can petition for removal based on new information such as a change in foreign sourcing, technological advancement, etc.

We note that with such an expansion of the export control regime additional resources may be necessary. We recommend the Secretary of Commerce request, and Congress provide, additional resources to support the continuous review of U.S. export controls. As Commerce develops the Rule for consideration, it would be helpful for the Department to evaluate resource requirements to manage the new regime and communicate those requirements to relevant stakeholders.

Comments on Specific Technologies

As reflected below, ITI received feedback on a number of technologies listed in the ANPRM. We would note that our submission is not a complete list of technologies ITI companies develop and/ or utilize. The following reflects examples that could be collected in the limited time allotted. To that end, we recommend BIS conduct additional outreach to industry to better understand the relative maturity, and specific history of, innovation in particular fields.

Artificial Intelligence

Artificial Intelligence (AI) and machine learning (ML) today are considered within the tech sector to be mainstream and widely available technology categories in the United States and foreign countries –which do not fall neatly into an "emerging" or "foundational" technology definition. AI technologies include, but are not limited to: natural language processing, virtual assistants, robotic process automation, unique identity, and video analytics. Investment in AI has increased rapidly with advancements in computing power and data availability over the last decade. The basic algorithms and methods enabling such capabilities are not new or "emerging"; the field has existed for over 50 years and even specific techniques in machine learning, such as deep learning, which has been central to many of the most impactful AI applications thus far, were breakthroughs achieved in the 1980s.

A reasonable analogy for AI today would be mass electrification. As noted in a recent *Wired* story, Thomas Edison's harnessing of electricity, the field rapidly shifted from invention to implementation. Thousands of engineers everywhere began tinkering with electricity, using it to power new devices and reorganize industrial processes. Continued R&D in electricity continues to occur—like on

breakthrough battery power technologies. While those technologies have national security use, they are being driven largely by the private sector for commercial use—like in higher performing electric cars.

Examples of AI applications include: medical image analysis; navigation; self-driving cars; accessibility for visually-impaired people; language translation; natural language processing; fraud detection and payment processing; and security. Companies that develop networking solutions are also using AI and machine learning to build automated IT networks that self-configure, monitor, manage, correct, defend, and analyze data traffic with little human intervention. Automated networks will use machine learning to interpret vast amounts of traffic behavior data; predict performance issues before users are affected; and configure and deploy any necessary protections. Additionally, advances in hardware specialized for training and running ML systems have helped accelerate the development of such applications.

The leading companies, universities and researchers on these technologies are located not only in the United States, but also around the world, including in China, Singapore, the EU, Russia, and Canada. Because the core elements of AI- from computing to talent to data- are globally available and integrated into robust AI ecosystems in these markets in particular unilateral controls would risk disproportionately harming the U.S. AI ecosystem. Several well-funded Chinese computer vision companies (including SenseTime, Megvii Technology, CloudWalk) market leading-edge computer vision applications. For example, China's SenseTime is working to deploy their image recognition technologies into autonomous driving, smart city, and medical applications. Notably, in the most recent Face Recognition Vendor Test (FRVT) conducted by U.S. Department of Commerce, National Institute of Standards and Technology - the top teams hailed from China and Singapore. In the 2017 ImageNet competition, again, Chinese teams led the overall competition in object detection. This does not mean that the U.S. is "losing" the AI race; rather, it underscores the need for the U.S. to ensure its companies can develop and market their products by maximally leveraging the world's best talent and invest in the strengths of the U.S. AI ecosystem.

The U.S. faces significant global competition with regard to AI leadership and investment. In 2017, China attracted greater global investment in AI start-ups than the United States (48 percent compared to 38 percent) and published six times the number of AI and machine learning-related patents compared to the U.S. However, China is not the only country with the capacity to harness the economic benefits of AI technologies. An analysis of 12 different economies (excluding China) found that AI has the potential to double the annual economic growth rates in those economies and boost labor productivity by up to 40 percent by 2035. As other countries continue to prioritize AI development and deployment, unilateral controls could have a chilling effect on U.S. AI investment and innovation, and therefore U.S. global dominance on AI.

It is important to note payment systems rely on AI and machine learning to look for anomalous transactions patterns to detect and mitigate payment fraud. Additionally, the development of biometric recognition technology, such as facial, fingerprint, and voice recognition, is more effective in authenticating account holders, and any export control restrictions should distinguish between

biometric technology that is used for surveillance and biometric technology that is used for purely commercial purposes.

Additionally, companies that develop cybersecurity solutions would be affected by unilateral controls as they are currently exploring ways that AI can best be integrated into their products and services to defend against evolving threats. As cyber adversaries become increasingly automated, defense must also be automated and able to keep up with cyber attacks. Hindering the ability of U.S. cybersecurity solution providers to leverage AI technologies, for example to identify and patch vulnerabilities, weakens their ability to defend organizations globally – including U.S. government agencies, customers, partner entities, and supply chains – against cyber adversaries. To these points, we would urge BIS to exempt certain narrowly defined back-end data sets used by AI- and machine learning technologies from export controls, namely those used for cybersecurity purposes and that are not subject to ITAR or other existing US export controls. In the cybersecurity context, these technologies are only as successful as the data on which they rely, as this data enables critical pattern detection, conclusion drawing, and decision-making. Controls back-end data sets would significant increase costs and lower the efficacy of research needed for US firms to remain competitive in the global marketplace.

Position Navigation and Timing (PNT) Technologies

Position Navigation and Timing (PNT) Technologies are widely available outside the U.S. As you know, PNT technologies include a wide range from satellite technology, mapping, and related technologies. Furthermore, there are many services that use such technology even if they do not directly develop and operate the technology. U.S. companies must be able to use these technologies in global markets in order to remain competitive, particularly when it is necessary to pair with local partners. For example, the payments industry uses location technologies to help ensure the security and integrity of payment transactions and to provide ATM Locator services around the globe.

Microprocessor Technology/System-on-Chip (SoC)

The microprocessor technology, System-on-Chip (SoC), is the high integration of many functions on a single chip. This is made possible with the fast progress of transistor technology and lithography keeping pace with Moore's Law. The integration of AI accelerators into an SoC – called AI-Chips – have proliferated with large dollar investments made in semiconductor industries, including in the U.S., Europe, and China, to accelerate many of the AI applications. In fact, SoC's are in wide production around the world. New "technology" U.S. export controls on this widely adopted technology will adversely impact U.S. companies, providing an advantage to foreign competitors.

Broad new controls on microprocessor technology could have a negative impact on the design, development, and/or production of microprocessors as SoCs today are in world-wide production. These new emerging technology controls would adversely impact U.S. companies involved in this industry, including the electronic design automation (EDA) industry. For example, the EDA industry's competitiveness, revenue, operations, workforce, and research and development would be negatively impacted. A conservative estimate of the impact of implementing controls would be a loss of revenue of approximately USD $5 million-$10 million or more per chip in IP and EDA, while customers could look to foreign firms (such as a third-party ASIC design firm) or a foreign IP supplier

to source the required tools and IP. The availability of finished microprocessor products for use in IT equipment around the world is critical to any U.S. business with global operations. Any controls should continue to ensure that U.S. businesses can deploy those products.

Given this is not an emerging technology, we do not believe any controls are appropriate. Indeed, such controls would affect the ability of U.S. companies to continue to play a central role in the development of harmonized global standards, including in areas such as the standards applicable to chips used in payment cards. Such activities help ensure that U.S. companies continue to play a leading role in global commerce.

Data analytics

Development of data analytics technology is truly global in its nature. One key application area of data analytics technology is related to cybersecurity. Network security companies develop and deploy data analytics toward malware, malicious IP addresses, and other cyber threats. The goal of this is to collect and analyze cyber threat indicators to understand how the threats evolve, what they are targeting, and how to protect against them.

Restricting the export of data analytics technology would have a significant negative impact on global cybersecurity and cybersecurity cooperation. The White House has made it a priority to enter into cybersecurity cooperation agreements with governments around the World. For instance, in September 2018, the U.S. Ambassador to Indonesia and the Indonesian government signed a letter of intent related to cybersecurity cooperation. In August 2018, Defense Secretary James Mattis and his Chilean counterpart signed a cybersecurity cooperation agreement. Cybersecurity and cybersecurity cooperation require the data analytics tools to collect and analyze threat information.

Outside the cybersecurity context, however, data analytics tools are used for a wide variety of market research, fraud detection, and other purposes. For example, in the payments space, data analytics technology is a critical tool to ensure a safe payment network and helps provide valuable market research. Overly broad restrictions on the deployment of these technologies could cripple the ability of U.S. companies to provide these services. Data analytics are an important tool for uncovering widespread, large-scale criminal activity in the payments sector, and curbing the deployment of such technologies could limit the ability of the financial industry to report suspicious transactions thus having a detrimental impact on law enforcement.

Quantum Information and Sensing Technology

Quantum technology is critical to the future of many U.S. businesses, and it will be necessary to deploy this technology in markets around the world in order to remain competitive. As a fundamental different approach to computing with theoretical limits that surpass classical computing in significant ways, the positive potential and range of applications cuts across nearly every sector of the economy. The ability to deploy quantum technology around the world will be particularly important to combat criminals who may have the ability to employ powerful technologies to decrypt and illegally obtain sensitive information, including financial information. For example, quantum encryption will be critical to protecting the integrity of payment transactions.

Logistics Technology
Logistics technology is a very broad area. Without the identification of more specific technologies in this category, the technology is not emerging. U.S. companies require the continued ability to deploy technology that is critical to the integrity of supply chains, including technology to track payments across the supply chain, and to protect against the introduction of counterfeit and other illegitimate goods into global supply chains.

Additive Manufacturing
For more than 30 years, the U.S. has been the technological leader in additive manufacturing through 3D printing. This fact alone reinforces the point that this is not an emerging technology. As more countries recognize how additive manufacturing can be applied to advance the next industrial revolution, several governments are aggressively investing in R&D and/or planning deployment of additive manufacturing hubs, including China, South Korea, Germany, Italy, and the United Arab Emirates. Placing additional technology controls on decontrolled printer hardware would be of little strategic value and could cause European and other manufacturers to design-out U.S. technology.

Any services provided by application engineers related to weapons or defense-related digital print instruction files would be currently controlled under the ITAR defense services provisions, which should prohibit inclusion in the new export control regime. Technology to produce any 3D printing materials of concern (such as certain powdered metals), are currently controlled under Category 1 of the Export Administration Regulations (EAR). Lastly, U.S. 3D printing companies screen customers against trade sanctions and entities lists to prevent technology from falling into the wrong hands.

Rather than impose counter-productive new technology controls, ITI encourages the U.S. government to take proactive "run faster" measures to accelerate 3D additive manufacturing in the United States by investing in education and workforce training measures, enacting procurement policies that mandate domestic 3D printing part purchases, creating tax incentives for U.S. companies using 3D printers to localize manufacturing to offset investment costs, and partnering with industry to ensure the existing legal framework provides IP protection for 3D printing.

Conclusion
Thank you for the opportunity to provide comments. As suggested above, the outcome of this process is of critical concern to all ITI member companies. It is important that efforts to strengthen national security be narrowly tailored to essential national security concerns so that U.S. companies can continue their global technology leadership, which is in and of itself an essential component of national security. An overly broad and cumbersome export control regime will disadvantage U.S. companies and harm the economy. We appreciate BIS's understanding of the need for a balanced approach and look forward to working with Commerce and other stakeholders as you develop these regulations.

Sincerely,

Jennifer McCloskey
Vice President, Policy