McAfee, LLC
2821 Mission College Blvd
Santa Clara, CA 95054
www.mcafee.com

January 10, 2019

VIA ELECTRONIC SUBMISSION
***Regulations.gov* Docket Number BIS-2018-0024**
Ms. Kirsten Mortimer
Office of National Security and Technology Transfer Controls
Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Avenue NW
Washington, DC 20230

Subject: RIN 0694-AH61

RE: Review of Export Controls for Certain Emerging Technologies

Dear Ms. Mortimer:

On behalf of McAfee, LLC ("McAfee"), thank you for the opportunity to provide comments on the advanced notice of proposed rulemaking (ANPRM) issued by the Bureau of Industry and Security (BIS) on November 19, 2018 concerning criteria for identifying emerging technologies that are essential to U.S. national security under the Export Administration Regulations (EAR).[1]

I. Overview

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions from device to cloud that make the world a safer place. By building solutions that work with other industry products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and

[1] 83 Fed. Reg. 58201.

collaboratively. We secure their digital lifestyle at home and while on the go by protecting consumers across all their devices and in the cloud. Working with other security players, we are leading the effort to unite against state-sponsored actors, cybercriminals, hacktivists and other disruptors for the benefit of all. McAfee is focused on accelerating ubiquitous protection against security risks for people, businesses and governments worldwide. Security technologies from McAfee use a unique, predictive capability that is powered by McAfee Global Threat Intelligence, which enables home users and businesses to stay one step ahead of the next wave of viruses, malware and other online threats.

In the ANPRM, BIS identified several representative technology categories that it stated may be important for U.S. national security and should possibly be controlled as sensitive "emerging technologies."[2] These included products and technologies of specific interest to McAfee, such as artificial intelligence (AI) and machine learning, AI cloud technologies, and certain advanced computing technologies.[3] BIS further requested that industry provide comments on how to define emerging technologies, the status of development of these technologies in the United States and other countries, the impact that imposing new specific emerging technology controls would have on U.S. technological leadership, and other approaches to the issue of identifying emerging technologies, including the stage of development or maturity level of an emerging technology that would warrant consideration for export control.[4]

II. BIS Should Take A Cautious, Do-No-Harm Approach to Identifying and Imposing Additional Controls on Emerging Technologies

As discussed in greater detail below, McAfee urges BIS to take a cautious, targeted, do-no-harm approach to identify potential emerging technologies. BIS should seek to impose only those controls that are critically necessary

---

2 *Id.* at 58202.
3 *Id.*
4 *Id.*

to preserve U.S. national security without unnecessarily burdening U.S. industry or stifling innovation.

In many cases, the technologies preliminarily identified by BIS in the ANPRM are actually in widespread use and well understood across the globe. Attempting to impose additional export controls on these technologies would, without a carefully targeted approach, harm only U.S. industries, U.S. innovation, and U.S. competitiveness while doing nothing to protect U.S. national security.

In addition, BIS should take care to ensure that technologies such as cybersecurity items should continue to be managed through existing BIS unilateral and multilateral control regimes and should not be intermingled with new controls on emerging technologies. For example, McAfee understands that BIS intends to continue to pursue issues raised in connection with its 2015 proposed rule on cybersecurity items[5] through a separate process of notice and comment rulemaking and possible future changes to the Wassenaar Arrangement multilateral controls. McAfee urges BIS to follow that separate and distinct track going forward and to continue to take the views of affected U.S. companies into account in that process. As it does so, BIS should avoid inadvertently conflating efforts to examine the utility and scope of multilateral controls on cybersecurity items with efforts to define and control emerging technologies.

Indeed, given the global availability of cybersecurity tools, many of which make use of the emerging technologies under review, McAfee respectfully submits that great care needs to be taken by our government before imposing additional export controls on American cybersecurity companies. Such rules could have the unintended and harmful consequence of stunting the growth and technical capabilities of the very companies that currently protect vital U.S. critical infrastructure, including federal and state government infrastructure, from cyber-attacks. Placing additional limitations on the ability of U.S. companies to compete for global markets with foreign

---

5 *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, 80 Fed. Reg. 28853 (Dep't Commerce May 20, 2015) (proposed rule).

companies that have made investments in many of these same cybersecurity technologies could stifle U.S. technological leadership and harm U.S. national and economic security.

Our nation's security progressively depends on our ability to stay ahead of aggressive nation state hackers. We can only achieve this objective by protecting our nation's industrial base of cybersecurity companies that require global markets to fund the research and development needed to stay on the cutting edge of technology innovation cycles that move at a rapid rate. These innovation cycles are in fact speeding up, as hackers leverage cutting edge innovations to defeat cyber defenses that often become obsolete in 12 to 18 months. McAfee thus encourages BIS take into consideration the global nature of our industry and the competitive technology environment in which we operate before adding new categories of emerging technology controls that could negatively impact U.S. technological leadership.

In the wake of the release of its 2015 proposed rule on cybersecurity intrusion and surveillance systems, BIS appeared to recognize that such considerations warranted a careful and limited approach to further regulation in this area. The decision to reconsider the proposed rule, and to seek to further narrow the scope of any additional cybersecurity-related export controls through multilateral efforts such as the Wassenaar Arrangement was, in the view of McAfee, the correct one. The United States should continue these efforts on a separate track and not include them in the scope of this rulemaking proceeding.

Moreover, BIS should remain cognizant of the fact that software-based technologies such as much of the technologies behind AI, data analytics, and machine learning are, by their very nature, fundamentally different from physical items and physical process technologies. Their intangible, readily-reproducible character makes software-based technologies inherently difficult to define and control. Unlike technologies such as nuclear technology where material can be physically controlled, or semiconductor technology that requires high-tech manufacturing processes and machinery to implement and use, software based technologies like AI or data analytics can be spontaneously created and deployed on existing systems and

networks without any additional physical inputs or physical processes. As the history of export controls on encryption software and encryption technology illustrate, attempts to control the transfer of software-based technology is inherently challenging and extremely costly in terms of government resources and the burden on industry. This history demonstrates that the enormous opportunity cost and vast government and industry resources required even to attempt to control software-based technology can and should be better spent on ensuring that companies can control and safeguard the IP that uses the technologies. Rather than burdening U.S. software companies with new and substantial export control compliance costs, the United States should seek to empower those companies to better protect themselves from forced technology transfers, data localization, IP theft, and other harmful policies and practices.

III. BIS Should Avoid Imposing New Controls on Technologies that Are Widely Available Outside the United States

Many of the "representative technology categories" identified in the ANPRM consist, in large part, of technologies that are widely available outside the United States. McAfee submits that imposing broad, unilateral export controls on these technologies would place U.S. companies like McAfee at a significant competitive disadvantage, while doing little to nothing to advance legitimate U.S. national security aims.

For example, foreign companies have made great strides in developing or bringing to market technologies that make use of back-end data sets needed to drive innovation in AI and machine learning as well as subcategories such as deep learning and natural language processing. Indeed, our nation's peer and near-peer technology competitors – Russia, France, China, and the UK – have either leading or rapidly improving positions in the emerging technologies under consideration. Accordingly, it is simply too late to attempt to prevent the spread of these technologies overseas. They are already "out there" and improving all the time, as the following examples illustrate:

- ***Russia.*** Russia reportedly spends an estimated $12.5 million annually on AI. However, the actual scope and extent of existing AI-based

technology in Russia is reported to be much larger due to Russian-government directed public-private partnerships.[6] As a result, Russia already has the policies and access to AI technology that will available to it to continue to make advancements in AI applications.

- ***China.*** According to experts such as Dr. Kai-Fu Lee, the author of the recent book *AI Superpowers: China, Silicon Valley and the rest of the World*, China has quickly closed the gap with the United States in AI. Dr. Lee's extensive research found that currently, there is near parity in many critical AI technologies between the United States and China. For example, China and the United States are tied in Internet AI, while China leads in Perception AI. Owing to the significant investments the Chinese government has made in AI research and broad-based tech training, Dr. Lee believes that China will further surpass the United States in both Internet AI and Perception AI and achieve a similar level of capability in in Autonomous AI within five years. Reflecting these advances, China is now in the process of implementing advanced Perception AI systems developed on its own initiative and with its own resources.[7]

The situation is similar for the "quantum computing" category identified in the ANPRM. In quantum computing, the E.U., Canada, Australia and the U.K. are all investing in developing quantum technologies – and are potential sources for U.S. collaboration – but they do not match China's scale of investment. China has already developed the first satellite capable of intercontinental quantum cryptography and has made leadership in quantum computing a national priority. According to research done by Alison Snyder of Axios, "The race to build a quantum economy," China is reportedly investing $10 billion in a Los Alamos-esque National Laboratory for Quantum Information Science, slated to open in 2020.

---

6 *See* Samuel Bendett, "Here's How the Russian Military Is Organizing to Develop AI," *Defense One* (July 20, 2018), *available at* https://www.defenseone.com/ideas/2018/07/russian-militarys-ai-development-roadmap/149900/

7 *See, e.g.*, "China's Surveillance State Should Scare Everyone," *The Atlantic* (February 2, 2018), *available at* https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/

In addition, Chinese companies are investing heavily in quantum computing and attracting top researchers from around the world. Some Chinese firms now have similar levels of human resources, access to capital, and market valuations as their U.S. and E.U. counterparts. The days of Chinese firms simply bolting electronic components together for American firms is now long gone.

Once again, the case is the same for the category of "data analytics technology" identified in the ANPRM. While American technology companies such as Google and Microsoft retain leading positions in data analytics, Chinese companies are making rapid strides, largely due to speed with which Chinese consumers have adopted E-Commerce. According to McKinsey's 2016 China consumer report, China is the world's largest e-commerce market, with 700 million e-commerce consumers, that generated $615 billion in 2015. This level of economic activity is on par with the economies of Europe and the United States combined. Moreover, Chinese tech companies have access to large amounts of customer data that are the new "oil" of the global economy. These data are made that much more valuable by the use of data analytics to gain insights into consumer buying habits. Chinese technology companies have made heavy investments in data analytics to help monetize the world's largest E-Commerce market, China. Through these efforts and investments, China is quickly achieving parity and in some cases taking a leading position in data analytics.

As a result of the widespread foreign availability of technologies like AI, quantum computing, and data analytics, as well as the continued investments in these technologies by companies and governments overseas, any attempt to impose unilateral U.S. export controls on technologies as a broad category or set of categories is almost certain to fail. It is, moreover, unlikely to deter the continued use and development of these technologies outside the United States.

The only likely result is to put U.S. companies like McAfee at a disadvantage, further threatening the U.S. industrial base and ability to innovate. Indeed, all of these technologies support the cutting-edge innovations that McAfee and other companies need to stay competitive in the global marketplace. The

more barriers that are placed between the United States and the continued foreign advancement and research in these technologies, the greater the risk that the United States falls further and further behind.

IV. Conclusion

Rather than attempting to shut the proverbial barn door after the horse has bolted, the United States should instead seek to build a community of like-minded partners to identify and implement a multilateral set of narrowly-tailored controls on specific applications, end uses, or end users that may pose national security concerns. The "representative technology categories" in the ANPRM such as AI, quantum computing, and data analytics are simply too broad to allow for such an approach. In fact, for any technology that has a significant range of potential applications and is already widely available overseas, a category-based, unilateral approach to export controls, however narrow, is likely to fail. This is particularly true for software-based technologies that are already in widespread use and under further development in multiple countries around the world simultaneously.

Instead of a categorical approach to export controls on emerging technologies, the United States should:

- Consider the use of existing mechanisms like the Entity List and Unverified List to provide targeted and highly-specific restrictions on a limited set of end users of concern;

- Work with key international partners to identify and impose appropriate multilateral controls on specific and carefully-targeted technologies and end uses in such a way as to allow continued, unimpeded trade and development efforts between and among these partners while restricting access to these technologies by persons who seek to undermine U.S. national security;

- Support U.S. companies' research and development efforts in new and emerging technologies while at the same time pushing back against forced technology transfers, data localization requirements,

and other policies and practices that impair the legitimate protection of trade secrets and intellectual property; and

- Ensure that efforts to regulate cybersecurity technologies do not impinge on the ability of U.S. cybersecurity companies to continue to innovate and remain competitive in the global marketplace. In this regard, continued evaluation of export controls on cybersecurity technologies should remain separate from the instant rulemaking process on emerging technologies.

* * *

Thank you again for the opportunity to comment on this issue of critical importance to our company and industry. If you have questions or require further information, please call me at (301) 613-3966 or send an email to thomas_gann@mcafee.com.

Sincerely,

/s/ Tom Gann

Thomas Gann
Chief Public Policy Officer
McAfee, LLC

Cc: Liz McCarron, Vice President, Deputy General Counsel and Chief Compliance Officer, McAfee, LLC