9 January 2019

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

RE: Review of Controls for Certain Emerging Technologies (RIN 0694-AG61)

To Whom It May Concern:

We thank you for the opportunity to provide the following comments in response to the Department of Commerce's call for input on criteria for defining and identifying emerging technologies, as well as other factors related to emerging and foundational technologies. Representing approximately 180,000 IEEE members in the U.S., the Institute of Electronics and Electrical Engineers – USA (IEEE-USA) is the largest professional society for the advancement of technology in the U.S. A large contingent of our membership in academia, industry, and commercial services are innovators and developers of emerging and foundational technologies, some of which may be covered under the current Export Control Reform Act.

The IEEE-USA recommends to BIS that it carefully evaluate the benefits of restricting access to emerging technologies against the risk of not realizing the societal benefits of releasing those technologies. In 2010, the Department of Commerce's Emerging Technology and Research Advisory Committee (ETRAC) stated, "To remain the technological leader in the 21st century, it is imperative that the U.S. simultaneously enable scientific discovery, promote economic growth, and preserve national security." Despite the globalization of information and technology, the primary constraint on leadership in technology remains a country's willingness to invest in new technologies, rather than access to the foundational technologies that are essential for discovery science. In other words, America's long-term global competitiveness will be harmed more by a decline in our own commitment to developing new technologies, than by other countries' access to advanced research. With the rise of a competitive China, ETRAC's message is even more valid today than it was eight years ago.

The Export Control Reform Initiative of the past Administration reduced some of the export control regulatory burden on industry. However, the reforms fell short of protecting what really matters by continuing to regulate technologies that are outdated or subsumed by contemporary technologies. The sale of encryption technology, for example, was heavily restricted long after the basic technology became commercially available all over the world.

IEEE-USA | 2001 L Street, N.W., Suite 700, Washington, D.C. 20036-4928 USA
Office: +1 202 785 0017 | Fax: +1 202 785 0835 | E-mail: ieeeusa@ieee.org | Web: http://www.ieeeusa.org

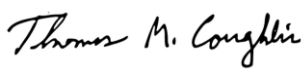
Such restrictions do not enhance America's national security, but do cost us technological innovations as American companies are passed by less restricted rivals.

In today's environment of mass murders, terrorism, and war, technology restrictions and export controls are still central to countering proliferation of those technologies that can increase the devastating effect of attacks on civilians, our freedoms and our society. Nevertheless, at present the United States government continues to guard both toothbrushes and diamonds with equal zeal, while new technologies are emerging that pose unique and troubling threats to that security.

IEEE-USA would be happy to answer any questions you might have regarding our analysis or suggestions. We further offer to provide subject matter experts to assist in the development of these definitions, including leaders in fundamental research and technology development.

Feel free to contact IEEE-USA's Government Relations Director, Mr. Russell Harrison, at (202) 530-8326 or r.t.harrison@ieee.org, if we can be of further assistance.

Sincerely,



Thomas Coughlin
2019 IEEE-USA President

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

The definition of emerging technologies varies across industry due to differing priorities of developer/manufacturer implementation or industry adoption. In some cases, the term is used to define a desired future technology. In other cases, the term applies to a market that is developing.

There are several definitions for emerging technologies that are often determined by the anticipated timeline for initial product realization resulting from research and development phases:

- Some industry investment firms define emerging technologies as those that have recently entered the market, but for which market growth has not yet peaked (i.e., not reached the peak of the hype curve.) For the context of this letter, we refer to these as "emergent technologies"
- In the eyes of many industry investments firms, emerging technologies generally encompasses technologies that would enter the marketplace within 5 years. These technologies are often at moderate technical readiness levels (4-7) and are developed with specific applications or commodities in mind.
- For venture/angel capital investors and some risk-tolerant investment firms, the horizon for emerging technology's realization is often extended to 5-10 years for moderate-to-high risk investments. These technologies are developed with some general concept of a commodity in mind, are at low technical readiness levels, but are beyond the basic research phase (i.e., technical readiness levels greater than 2).
- The defense or intelligence communities attempt to anticipate emerging technologies that are "over the horizon" of 10 years, sometimes referred to as "moon-shot" technologies. Their need to identify over-the-horizon technologies is predicated on their need to either exploit those technologies for a national advantage or develop suitable technical measures or tactics that can counter foreign emerging and disruptive technologies. These technologies are generally in research phases (TRL 0-2) and only broad concepts of applications are in mind.

In the context of export controls, the IEEE-USA recommends defining an "emerging technology" as a technology that is currently under development, reasonably expected to be available within the next five to ten years, and expected to have significant socio-economic or military effects.

One complexity within export controls is the current Bureau of Industry and Security definition of the word "technology," (Part 772, page 42, of the EAR), which states "Information necessary for the "development," "production," "use," operation, installation, maintenance, repair,

overhaul, or refurbishing … of an item." Simply adding the word "emerging" to the beginning of this definition will almost certainly have disastrous impact on fundamental research and innovation at universities and government or private laboratories because of its more specific implementation of the six constituent terms for BIS's active definition of "use" technology (operation, installation, maintenance, repair, overhaul, and refurbishing). Therefore, **IEEE strongly advises against this potential simplification.**

While protecting the United States from the loss of critical technologies is a worthy and important goal, it is not the only goal that must be considered. America's long-term prosperity depends on security today, but also the innovations, ideas and inventions that will protect us in the future, which is why fundamental research is so important, and so important to protect.

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

IEEE-USA recommends that BIS carefully weigh the risks against the benefits of the release of technologies. This analysis should include, but not be limited to, the following criteria for special emerging technologies of unique importance to national security:

1. Emerging technology with significant potential to pose a military or intelligence threat because it:
   - Introduces an asymmetry in modern U.S. warfare;
   - Negates or significantly diminishes the effect of significant American or its allies' hardware or tactics that – if implemented – would afford distinct military or intelligence advantage;
   - Significantly reduces the chances that the U.S. or its allies will authorize use of certain weaponry or intelligence tactics; or
   - Subverts U.S. or allied defensive systems.

2. Emerging technology with significant potential to pose an economic threat to the U.S. because that technology has the ability to:
   - significantly harm critical infrastructure;
   - disrupt vital communications platforms;
   - disrupt, damage, or destroy financial infrastructures; or
   - significantly reduce U.S. economic competitiveness if implemented by a foreign actor.

Focusing on a list of technologies alone without providing the criteria for establishing what state of the art will be subject to control makes the list a threat to U.S. enterprises. Any discretion in the interpretation of a technologies' inclusion on the list would impose cost, uncertainty, and barriers to entry to U.S. firms seeking to participate in global markets.

The list of technologies contained in the ANPRM is overly broad. The technologies listed are almost all fundamentally dual use and capture large swaths of technology that are not specific to America's economic and military advantage.

Requiring licensing for this large class of technologies will create an unacceptable burden on academic and industrial users of these technologies, restricting the ability of U.S. researchers and entrepreneurs to compete in global markets and leaving an unimpeded advantage to foreign economic and technical competitors who do not face the burden of these restrictions.

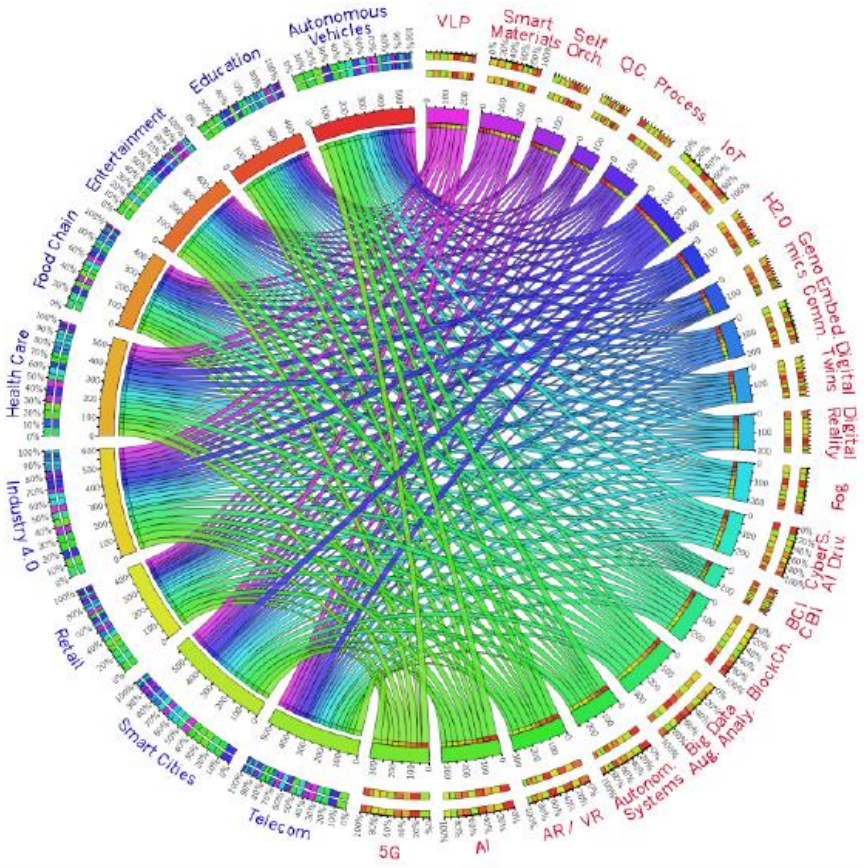
The divergent security implications of these technologies are significantly unclear - for example the imaging sensors produced globally for inclusion in mobile telephones today far outstrip the quality of military sensors available just a short time ago and are available at a price point a fraction of what was charged for military devices. Moreover, these sensors enable image-processing capabilities that clearly have security implications. Putting the genie back in the bottle is impossible, but locking American engineers out of global markets can happen quite easily.

Many of the technologies listed (for example all of the AI technologies) are about algorithms and software. Restricting export of these items has proven impossible in the past (as was the case with encryption technology), and will serve only to burden America academics, researchers and entrepreneurs.

Finally, the list presumes that the U.S. has an existing advantage in these areas. In areas where the U.S. has already ceded manufacturing and technology advantage to other countries, locking U.S. academics and entrepreneurs out of the exchange of ideas will further diminish American capabilities, rather than protecting them.

Sources to identify such technologies:

Every year, the IEEE Future Directions Committee performs forward-looking analysis by polling senior technical leaders in industry for their insights on near-term and long-term emerging technologies. The data from these studies is used to guide IEEE investments and efforts in its own future directions. As example of the form of analyses that the IEEE produces is shown below.



Similar to IEEE, many professional engineering and scientific societies and the National Academies maintain a high degree of awareness of technology trends that extend beyond 5 years. We, therefore, suggest that the BIS involve representatives from these organizations for initial emerging technology identification. After identifying the candidate technologies, the BIS should use its Emerging Technologies Technical Advisory Committee and interagency partners to evaluate and monitor their technological maturity.

Commercial technology forecast services, although expensive, are conducive for identifying and gauging maturity of technologies that are close to emergence. Many services use bibliometric or scientometric techniques that are derived from market analysis, patents and sometimes scientific literature. However, the predictive capabilities of these techniques vary greatly by technical discipline and the degree to which proprietary information might be protected. For example, a large electronics manufacturer might initiate basic research, but prevent publication or patents for several years until 6-12 months before marketing its next generation product – that is to say, these are *emergent technologies*. Another example would be the pharmaceutical industry where the full research, development, testing, evaluation, and final approval cycle is closely held for 12-15 years until months before product release in order to ensure competitiveness and return-on-investment. These short-time characteristics could inhibit BIS from having ample time to properly institute a control.

In addition, scientometrics often miss convergences between differing technology areas that may enable emerging technologies. While tools exist to identify such convergences, the strongest indicators tend to be topical areas pursued in research proposals at large-scale, multidisciplinary institutions like universities, government or private industry laboratories. By examining both winning and unfunded proposals for potential future technology areas, BIS would likely have insight into technologies that would emerge in the 5-10 year timeframe.

And, finally, the Intelligence Advanced Research Projects Agency (IARPA) invested in a crowd sourcing tool, called *CREATE (Crowdsourcing Evidence, Argumentation, Thinking and Evaluation)*, which solicited input from the general public on various analytic reasoning topics. BIS should consider adapting this tool for technology forecasting with a "trusted" community of volunteer scientists and engineers that would help with identification and potentially refine the risk-benefit analyses of emerging technologies.

Other general technology categories that warrant review to identify emerging technology that are important to U.S. national security:

1) Quantum Information Sciences:
    i. Quantum sensing
    ii. Quantum Radar
    iii. Fermionic sensors as gravimeters, magnetometers, antenna
2) Biotechnologies:
    i. Chemically-enhanced RNA modification/modulation
3) Remote sensing:
    i. Ultra-low light vision,
    ii. Remote neutron or gamma-ray detection from small, unmanned aircraft or low-earth orbit cube-sats
4) Under Artificial Intelligence:
    i. Methods for engendering user trust of AI
    ii. AI-assisted data analytics could assist
    iii. AI-implemented cyber-defense systems
5) Position, Navigation, and Timing (PNT) technology.
    i. Atomic clocks (chip-scale atomic clocks CSAC) and atomic-sensor-based navigation technologies
    ii. Chip-scale optomechanical oscillators as gyroscopes
    iii. Fermionic sensors
    iv. Nano-gravitometers
    v. atomic-magnetometers

6) 3D Printing Technologies
    i. 3D bioprinting dual-use technologies.
    ii. Additive manufacturing of explosives and pyrotechnic components
    iii. Additive manufacturing of nuclear materials and components or materials processing
    iv. Mobile additive manufacturing systems for vehicle components
7) Advanced Materials:
    i. Applications of microreactors for materials processing
    ii. Metamaterials;
    iii. Shape-memory polymers
    iv. Smart materials (materials that adapt or respond to surrounding environments)
8) Control systems:
    i. AI-assisted, self-correcting control algorithms
    ii. Augmented reality systems

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

At the time that export controls were codified into American and international laws, there were very few countries that could match the science and innovation prowess of the U.S. Today, the world is very different. The globalization of access to information and increased investments from other countries in fundamental research has eroded U.S. leadership in several key technological areas, including, but not limited to: genetic sciences, public health, optics, advanced materials development and crystal-growth, space exploration, quantum information sciences, artificial intelligence, and high performance computing.

For example, China (America's most alarming competitor) became Europe's largest supplier of technologies in 2013. Despite lagging slightly in total citations – a generally-accepted measure of quality - China passed the U.S. as the largest producer of peer-reviewed scientific and engineering literature in 2015, and has continued to increase its publications at an unprecedented rate.

Given the limited time of the Request for Information, an exhaustive analysis of international progress in each of these technical areas is not possible here. However, IEEE along with many of its peer societies and the U.S. Intelligence Community likely have the ability to compile these data for BIS.

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

In the opinion of IEEE-USA, specific controls over emerging technology could undermine U.S. technological leadership. BIS exploration of the *D521 "holding ECCN" had mixed results, for

example. The creation of this ECCN was intended to provide BIS with sufficient time to propose multilateral controls and/or implement export control regulations. Broad categories were listed including biosensors-on-a-chip and autonomous-control systems for UAVs; however, the specifications for the technologies being regulated were nonspecific and nebulous.

Several universities refrained from or rejected contracts with USG entities when proposed research fell into *D521 ECCNs because of concerns over implications of deemed export regulations and their potential application to the research. Furthermore, Dual-Use Research of Concern subjected formerly uncontrolled, fundamental research to Deemed Export controls. In both cases, many universities remain focused on research that is freely and openly discussed and publishable without restriction - while tending to avoid approving contracts for technologies that are potentially subject to deemed export regulations.

This example highlights the need for a clear, narrow and well-defined criterion to identify specific technologies for control.

Criteria for defining and identifying emerging technologies

The historical process of the Bureau of Industry and Security has been to develop and deliver technology export control proposals to multilateral regimes. In recognition that, according to BIS officers, this process takes 2-3 years from initial conception to implementation, the IEEE-USA suggests that BIS focus efforts on technologies that will emerge within the next 5 - 10 years.

In identifying emerging technologies, the IEEE-USA recommends that BIS request analysis from the U.S. Intelligence Community, industry representatives, and professional associations that carefully weighs the societal (economic, health, goodwill, etc.) benefits against the release risks (military, intelligence, economic, or global security) of a specific technology. These risk-benefit studies should, at a minimum, include quantified benefits analysis as well as likelihood-consequence risk estimates. The estimates should stretch beyond projections of casualties or potential earnings, but rather include estimations of short-term and long-term impacts across a broad spectrum of socio-economic factors.

We recommend that these estimates use a scale standardized for threat assessments by the U.S. Government, such as “None – Minimal – Moderate – Severe – Grave” for consequence and “Low – Moderate-High” for likelihood. We recommend that only those technologies that carry a threat level of “severe” or higher consequences and “moderate” or higher likelihood be eligible for unilateral controls should multilateral regimes not be achievable; while “moderate” or higher consequences with low or higher likelihood should only be considered with multilateral regime controls.

Furthermore, the analyses should carefully delineate the specific “risk-enabling characteristics” from the “benefit-enabling characteristics” of the emerging technology (i.e., foundational technology) in order to define bright-lines that distinguish the potential applications. Using this information, BIS must then evaluate whether the identified foundational/emerging technologies are uniquely under development within the U.S. or are being competitively sought by other countries with or without regulatory restrictions.

The IEEE-USA recognizes that our risk-benefit analysis recommendation is burdensome and would require a level of coordination that BIS currently has limited resources to support. However, as the BIS’s very own ETRAC pointed out with similar recommendations in 2013, the potential consequences of stifling innovation through emerging technology controls are very significant. In this era of globalized technologies and increased technological competitiveness around the world, it is far easier to out-innovate a potential adversary than to withhold access to emerging technologies. Similarly, regulating broad technology categories instead of defining distinct bright-lines in the U.S. could perversely result in promoting technological supremacy by an adversary.

As such, the BIS is firmly at the nexus of ensuring security from potentially dangerous technologies and ensuring the U.S. duly benefits from economically-impactful technologies. As BIS evaluates its process for identifying and regulating emerging technologies, we strongly recommend that the Department of Commerce, as a whole, also use this process for similarly identifying technologies that the U.S. Government should be investing in for the security of its industry and nation. Louis Pasteur rightly said, "Science knows no country, because knowledge belongs to humanity, and is the torch which illuminates the world. Science is the highest personification of the nation because that nation will remain the first which carries the furthest the works of thought and intelligence."

For America to remain competitive, we need to both protect key technologies and stimulate innovation to remain ahead. Similar to recommendations provided by the BIS’s former ETRAC, we recommend that any analyses that BIS performs on emerging technologies be shared with Small Business Investment Research program participants, as well as other government agencies that support fundamental research.

Input on Specific Technologies

The IEEE-USA recommends that BIS focus more effort on defining the characteristics of foundational technologies that must be protected for international security purposes than on emerging commodities.

For example, quantum computers offer a challenge that is typical of many emerging technologies. Quantum computing offers American businesses an enormous opportunity for growth, and offers American society innumerable potential benefits. But the technology could, in some cases, also be damaging to U.S. national security interests. Therefore, a careful balance must be reached between allowing the U.S. to realize the economic and societal benefits of quantum computing, while restricting access to the technology outside of the U.S.

Historically, export controls have referred to cutting-edge chip-scale, feature resolution, and processor speed as metrics for regulations. While similar characteristics are indeed feasible for quantum computers, the focus should be on what applications are of concern and what unique hardware characteristics are necessary to enable those applications.

Given the current emergence of quantum computing (e.g., Canadian manufacturer D-Wave), we recommend creating a panel from subject matter experts to define the technological characteristics that should be protected. IEEE-USA can provide specific recommendations on technical experts that may be able to assist in this technology area.

Such an approach would also work for software and cooling systems, each of which poses a major hurdle for space-efficient quantum computers. Software, in particular, that can effectively leverage the unique architecture and computing power of quantum computers currently lags the development of hardware, but is emerging at an unprecedented rate.

The characteristics of concern for both software and cooling systems should be identified by the panel mentioned above to ensure that the America's competitiveness in this emerging field is not inadvertently compromised, while still allowing for the protection of U.S. national security.