2020

Solving the Emerging Technology and National Security Conundrum

Shabbir Hamid

Solving the Emerging Technology and National Security Conundrum

BGN: 1.

TABLE OF CONTENTS

INTRODUCTION

The United States is known worldwide for its high quality, innovative goods and services,[1] and several businesses regularly export its products to other countries.[2] Although most products are not subject to export regulations, the government closely regulates several types of exports.[3] Academic literature has persistent and extensive discussions about what exports should be regulated and what trade policies should govern such regulation.[4] National security has long been a reason why exports are regulated.[5] For example, defense-related exports, or so-called "dual-use" technologies—those that can be used in military and civil functions—have long been

---

[1] *Export Planning*, INT'L TRADE ADMIN., http://apps.export.gov/article?id=why-export (last visited Aug. 2, 209)

[2] *Id*.

[3] *Id*.

[4] *See, e.g.*, Robert E. Klitgaard & Richard Huff, *Limiting Exports on National Security Grounds*, 4 COMM'N ON THE ORG. OF THE GOV'T FOR THE CONDUCT OF FOREIGN POL'Y 441 app. at 443 (1975) ("But critics of all stripes, as well as many officials now administering export controls, agree on one thing: *current policy and procedures are in a shambles*"); *see, e.g.*, Trey Herr & Paul Rosenzweig, *Cyber Weapons and Export Control: Incorporating Dual Use with the PrEP Model*, 8 J. NAT'L SEC. L. & POL'Y 301, 320 (2016) (contemplating when malware becomes a weapon of war).

[5] *See* Jere W. Morehead & David A. Dismuke, *Export Control Policies and National Security: Protecting U.S. Interests in the New Millennium*, 34 TEX. INT'L L. J. 173, 186 (1999) ("Controlling the export of such weapons and the technology to make them has been the cornerstone of U.S. policy since the conclusion of World War II").

regulated by U.S. export controls.[6] However, in an era where technology develops so rapidly beyond comprehension, and certainly beyond efficient regulation, emerging technologies have become a moving target.

With China's economic growth and Russia's ever-looming threat, along with the recent history of technological attacks, bad actors are empowered to use new technologies against the U.S. Legal literature has discussed "emerging technologies" as a topic for a significant time.[7] Articles often use the term to describe the concept that regulations should match the challenge of meeting technology development.[8] Technology is evolving so fast that it is no longer possible for people to predict its future.[9] In other words, technology will continue to develop at a fast pace, and its regulation needs to keep up.

---

[6] *See infra* note 42.

[7] *See, e.g.*, Gregory N. Mandel, *Regulating Emerging Technologies*, 1 LAW, INNOVATION & TECH. 75, 92 (2009).

[8] *Id*.

[9] Chris Gulker, *Technology is moving so fast that we can no longer reliably predict the future even a few years ahead*, INDEP. (March 10, 1998), https://www.independent.co.uk/arts-entertainment/technology-is-moving-so-fast-that-we-can-no-longer-reliably-predict-the-future-even-a-few-years-1149323.html. It is a strange thought that this article was written before Apple introduced the first iPhone, which ushered a new era of mobile technology. *See* Ben Gilbert, *It's been over 12 years since the iPhone debuted–look how primitive the first one seems today*, BUS. INSIDER (July 22, 2019), https://www.businessinsider.com/first-phone-anniversary-2016-12 (addressing how technology has developed since the first iPhone).

Emerging technologies are compromising our national security. For example, Russia allegedly influenced the 2016 elections through Facebook's data technology.[10] China allegedly committed cyberattacks against universities to steal research on naval technologies.[11] Criminals are committing local "ransomware" cyberattacks through Eternal Blue, a technology created by the National Security Agency.[12] Compromises in national security due to the proliferation and malicious use of technologies have become a part of the regular news cycle. On a large scale, people with malicious intent could use technology to crumble economic infrastructures, disrupt social communications, or attack with technologically advanced military weapons.[13]

---

[10] Julia Kollewe, *Facebook Profit Likely to Fall After Fake News Privacy Scandals*, GUARDIAN (Apr. 22, 2019), https://www.theguardian.com/technology/2019/apr/22/facebook-profit-fall-fake-news-privacy-scandals.

[11] Shannon Liao, *Chinese hackers reportedly targeted 27 universities for military secrets*, VERGE (March 5, 2019), https://www.theverge.com/2019/3/5/18251836/chinese-hackers-us servers-universities-military-secrets-cybersecurity.

[12] Patricia Mezzei, *Hit by Ransomware Attack, Florida City Agrees to Pay Hackers $600,000*, N.Y. TIMES (June 19, 2019), https://www.nytimes.com/2019/06/19/us/florida-riviera-beach-hacking-ransom.html; Nicole Perlroth & Scott Shane, *In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc*, N.Y. TIMES (May 25, 2019), https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html?module=inline.

[13] *See, e.g.*, Michael Griffin, *The Dangers of Modern Technology*, ODYSSEY (Aug. 18, 2015), https://www.theodysseyonline.com/the-danger-in-modern-technology (commenting on the dangers of technology in context of cyberattacks); *see also*, Max Boot, *The Paradox of Military*

Oracle Corporation is a prominent provider of business software that has a significant role in the development of emerging technologies.[14] Edward Screven, Chief Corporate Architect of Oracle Corporation, noted the perils of working with data, "[W]e manage important data—critical data—for tens of thousands of customers today in our data centers across the world. And of course, there are a lot of bad actors out there, who would like to get to it, either to get the data, or worse, try to change it."[15] Similar to the national security concern that cloud data centers pose, other technologies, such as artificial intelligence, DNA manipulation, and 5G technology, have critical security implications. But since regulation cannot simply stop innovation and the development of technologies, identifying emerging technologies in a way that allows for efficient regulation is a critical challenge. It is also difficult to clarify what dangers emerging technologies could realistically have to national security.

Recently, in the John S. McCain National Defense Authorization Act for Fiscal Year 2019,[16] Congress called upon the President and the heads of his agencies to establish a process in which the heads of agencies conduct a regular, ongoing, process to identify "emerging and

---

Technology, NEW ATLANTIS J. OF TECH. & SOC'Y 13, 13–26 (2006), https://www.thenewatlantis.com/docLib/TNA14-Boot.pdf (commenting on the U.S. dominance over various military technologies).

[14] *Oracle Fact Sheet*, ORACLE (2019), http://www.oracle.com/us/corporate/oracle-fact-sheet-079219.pdf.

[15] *Emerging Technology Trends & National Security*, CTR. FOR STRATEGIC & INT'L STUD. (March 25, 2019), https://www.csis.org/events/emerging-technology-trends-and-national-security.

[16] 50 U.S.C. § 4817 (2019).

foundational technologies"[17] that "are essential to the national security of the United States."[18] The Act failed to define what national security is in this context. However, it described what the interagency process should take into account:[19] the development of emerging technologies in foreign countries, the effect of export controls on developing emerging technologies in the United States, and the effectiveness of export controls in limiting the proliferation of emerging technologies to foreign countries.[20]

In addition to these guidelines, the Act required a notice and comment period.[21] The Department of Commerce's Bureau of Industry and Security (BIS) initiated an advance notice of proposed rulemaking (ANPRM) seeking public comment on defining and recognizing emerging technologies that may have national security implications.[22] The goal behind recognizing these

---

[17] *Id.*

[18] *Id*.

[19] 50 U.S.C. § 4817 (a)(2)(B).

[20] *Id*.

[21] 50 U.S.C. § 4817 (a)(2)(C).

[22] This comment period does not include identification of "foundational technologies," for which a separate advance notice of proposed rulemaking (ANPRM) will take place. *See* Review of Controls for Certain Emerging Technologies, 83 Fed. Reg. 58,201 (Nov. 19, 2018) (to be codified at 15 C.F.R. § 744) (2018) (designating seven areas that comments should focus on: "(1) How to define emerging technology to assist identification of such technology in the future; (2) criteria to apply to determine whether there are specific technologies within these general categories that are important to U.S. national security; (3) sources to identify such technologies; (4) other general technology categories that warrant review to identify emerging technology that

emerging technologies is to make the export of such technologies subject to the Export Administration Regulations (EAR) by placing that product on the Commerce Control List (CCL).[23] The ANPRM suggested fourteen broad categories to help identify emerging technologies.[24] Through this ANPRM the BIS seeks to add technologies to this list, and place export controls on them.[25] Currently, exports are controlled via the CCL, through which the EAR, as a minimum control, issues licenses to exporters that want to ship an item on the CCL.[26] The BIS seeks to add newly identified emerging technologies to the list, and impose, at a minimum, a license control to the items on the CCL.[27]

---

are important to U.S. national security; (5) the status of development of these technologies in the United States and other countries; (6) the impact specific emerging technology controls would have on U.S. technological leadership; (7) any other approaches to the issue of identifying emerging technologies important to U.S. national security, including the stage of development or maturity level of an emerging technology that would warrant consideration for export control."

[23] *See id*; 15 C.F.R. §734 (2017).

[24] 15 C.F.R. § 744 (2018). The broad categories listed are biotechnology; artificial intelligence and machine learning technology; position, navigation, and timing technology; microprocessor technology; advanced computing technology; data analytics technology; quantum information and sensing technology; logistics technology; additive manufacturing; robotics; brain-computer interfaces; hypersonics; advanced materials; and advanced surveillance technologies.

[25] The ANPRM has now ended. Businesses and practitioners are still waiting for the Commerce Department to publish new rules.

[26] *See infra* PART TWO.

[27] *See* 15 C.F.R. §744 (2018).

Regardless of what rules the BIS adopt, the scope of national security seems ill defined and unclear.[28] The BIS needs to publish additional guidance describing when national security is implicated, with examples or realistic illustrations of national security being compromised that could be effectively avoided through export regulations. Also, the technological and business expertise of those who are attempting to adopt these regulations may be inadequate.[29] There is a fundamental disparity between the knowledge and expertise of the government and private corporations.[30] This process of adopting export regulations may hinder U.S. innovation and market interests because of its broad designations that may require a lengthy licensing process. Additionally, the process may also be too slow to react effectively and efficiently to technology's

---

[28] *See* Jay Stanley, *How to Think About the National Security State*, ACLU: FREE FUTURE (Sept. 5, 2013, 11:00 AM), https://www.aclu.org/blog/national-security/secrecy/how-think-about-national-security-state?redirect=blog/technology-and-liberty-national-security-criminal-law-reform/how-think-about-national-security (exploring why it is important to clearly understand national security, suggesting that it enables people to keep the leaders in check); *see also*, Jay Stanley, *The National Security State: Why it's Important to Understand the Nature of the Beast*, ACLU: FREE FUTURE (Sept. 10, 2013, 3:48 PM), https://www.aclu.org/blog/national-security/secrecy/national-security-state-why-its-important-understand-nature-beast?redirect=blog/criminal-law-reform-national-security-technology-and-liberty/national-security-state-why-its (commenting that there is a wall of secrecy behind which national security agencies operate).

[29] *See generally*, Harold H. Bruff, *Presidential Power Meets Bureaucratic Expertise*, 12 U. PA. J. CONST. L. 461 (2010) (discussing the role of expertise in bureaucracy).

[30] *Id*.

rapid development because it may always involve a reevaluation of new technologies through a comment period such as this one.

Part One of this Comment explains the definition of exports and the multiple agencies that have regulations for exports; Part One also discusses the role of the Committee on Foreign Investment in the United States (CFIUS) in export controls. Part Two explains the Export Administration Regulations (EAR), its process of exports regulation, and the types of products it currently controls. Part Three discusses the BIS's ANPRM on emerging technologies, including a brief discussion of comments made to the ANPRM. Part Four recommends a new rulemaking period to define the policy of national security to supplement identifying emerging technologies. Part Four also recommends creating a separate committee or agency to consolidate efforts in identifying emerging technologies.

PART ONE: EXPLAINING EXPORTS

A. Defining Exports

The EAR has defined exports on multiple facets.[31] Included in the meaning of an export is taking the item out of the country in any manner,[32] and transferring "technology" or source code to a foreign person in the United States is called a "deemed export."[33] Often situations arise where an item subject to the EAR is transferred from one foreign country to another foreign country.[34] Such a transfer is called a "reexport."[35] Release of "technology" to a foreign person

[31] 15 C.F.R. §§ 734.13–734.18 (2017).

[32] *Id*. at 734.13(a)(1).

[33] *Id*. at 734.13(a)(2).

[34] *Id*. at 734.14(a)(1).

[35] *Id*.

of another country is a "deemed reexport" to the foreign person's most recent country of citizenship or permanent residency.[36] When businesses want to export its products, they must first identify which agency's jurisdiction the product falls under. Then, the business must identify what classification of exports the product is subject to.[37]

B. Jurisdiction: Agencies that Control Exports

There are about sixteen agencies that have functions related to exports.[38] Three departments have broad jurisdiction over exports: the Department of State, the Department of Treasury, and the Department of Commerce:[39] The State Department has jurisdiction over defense related exports;[40] The Treasury Department's Office of Foreign Assets Control (OFAC) regulates transactions in administering U.S. economic sanctions.[41] The Commerce Department has jurisdiction over "dual-use" exports,[42] and other exports not identified by other agencies.[43]

---

[36] *Id.* at 734.14(a)(2). The EAR also defines other classifications that are similar to exports. *See id.* at 734.13–734.20 (defining release, transfer, export of encryption source code and object code software, etc.).

[37] *See infra* PART TWO (C).

[38] JOHN R. LIEBMAN, ROSZEL C. THOMSEN II, JAMES E. BARTLETT III & JOHN C. PISA-RELLI, UNITED STATES EXPORT CONTROLS §1.00 (7th ed. 2018).

[39] *Id*. at §1.01.

[40] Stanley J. Marcuss & Michael B. Zara, *A Better Way through the Export Control Thicket*, 14 SANTA CLARA J. INT'L L. 47, 48 (2016).

[41] *Id*.

[42] *See* 15 C.F.R. § 730.3 (2014) (defining dual-use exports as any item that has "civil applications as well as terrorism and military or weapons of mass destruction . . . applications.")

Although the agency's jurisdiction over an export often overlaps,[44] for certain "category-specific" items, one of these three agencies controls its export.[45] Other agencies have jurisdiction over specific exports. Some agencies, such as the Defense Technology Security Administration, Export-Import Bank, International Trade Administration, and U.S. Agency for International Development, provide advisory roles or policy-making roles over exports.[46] However, these agencies cannot regulate exports.[47] Other agencies, such as Customs and Border Protection and the Postal Service, serve administrative functions.[48]

Because so many agencies have overlapping jurisdiction, exporters have been consistently lobbying for the consolidation of these agencies.[49] Exporters, nonproliferation advocates, allies, and other stakeholders have criticized aspects of the export control system for

---

[43] Marcuss, *supra* note 40, at 49 (2016) (describing the jurisdiction of various export control agencies); *See* 15 C.F.R. §§ 772.1, 734.2(a) (2014) ("Exports under the Wassenaar Arrangement Munitions List (WAML) or the Missile Technology Control Regime Annex are also subject to the EAR"). The WAML is an international agreement through which participating States apply export controls to items set on an agreed upon "Dual-Use Goods and Technologies and Munitions" list. WASSENAAR ARRANGEMENT, https://www.wassenaar.org/ (last visited Sept. 20, 2019).

[44] Marcuss, *supra* note 40, at 49.

[45] *Id*.

[46] *Id*.

[47] *Id.*

[48] *Id*.

[49] *Id*.

being too "rigorous, cumbersome, obsolete," and inefficient.[50] Administrations have considered consolidation proposals, but no complete consolidation has happened.[51] The Obama Administration attempted to create a single licensing agency and merge the control lists to harmonize export control enforcement agencies, recognizing the inefficiency of the export controls system.[52] Currently, the Trump Administration is not pursuing agency restructuring in the same way the Obama Administration did, but is directing trade and export policies, especially with President Trump's stance on trade with China.[53]

---

[50] Ian F. Fergusson & Paul K. Kerr, *The U.S. Export control System and the Export Control Reform Initiative*, CONG. RES. SERV. 1, 1 (April 5, 2019), https://fas.org/sgp/crs/natsec/R41916.pdf.

[51] *See, e.g.*, Fact Sheet: Implementation of Export Control Reform, THE WHITE HOUSE (March 08, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/03/08/fact-sheet-implementation-export-control-reform (describing an initiative that is indicative of President Obama's export consolidation efforts).

[52] Fergusson, *supra* note 50, at 9–11.

[53] *See* Anna Fifield & David J. Lynch, *China warns of 'countermeasures' against U.S. products if Trump increases tariff*, WASH. POST (May 8, 2019), https://www.washingtonpost.com/world/asia_pacific/china-warns-of-countermeasures-on-us-products-if-trump-boosts-tariffs/2019/05/08/f45c6cb6-718e-11e9-9331-30bc5836f48e_story.html?utm_term=.b2e9aaf109c3; *but see* Control of Firearms, Guns, Ammunition and Related Articles the President Determines No Longer Warrant Control Under the United States Munitions List (USML), 83 Fed. Reg. 24,166 (May 24, 2018) (to be codified at

C. The Committee on Foreign Investment in the United States (CFIUS)

When mentioning the current status of exports regulation in the United States, a discussion of CFIUS is inevitable because it has a prominent role in controlling emerging technologies, but in a different manner.[54] Along with the jurisdictions of other export controlling agencies, the Foreign Investment Risk Review Modernization Act (FIRRMA) gave CFIUS expanded authority to analyze and monitor an extensive range of transactions by foreign investors in United States companies.[55]

CFIUS was originally established by President Ford's Executive Order[56] in 1975 to monitor the rapid increase of foreign investment by the Organization of the Petroleum Exporting Countries (OPEC) in American assets, specifically responding to concerns that OPEC's interests were not economic, but political.[57] After the enactment of FIRRMA,[58] the president is allowed

---

15 C.F.R. pt. 736, 740, 742, 743, 744, 746, 748, 758, 762, 772, 774) (consolidating exports controlled under the USML with the Commerce Control List, an export reform effort).

[54] *The Committee on Foreign Investment in the United States (CFIUS)*, DEPT. OF THE TREAS., https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius (last visited on Sept. 20, 2019).

[55] Harry Clark, *Ten Key Points About CFIUS and Export Control Reform*, ORRICK: INSIGHTS (Aug. 3, 2018), https://www.orrick.com/Insights/2018/08/Ten-Key-Points-About-CFIUS-and-Export-Control-Reform.

[56] Exec. Order No. 11,858, 40 Fed. Reg. 20,263 (May 7, 1975).

[57] James K. Jackson, *The Committee on Foreign Investment in the United States (CFIUS)*, CONG. RES. SERV. 1, 4–5 (May 15, 2019), https://fas.org/sgp/crs/natsec/RL33388.pdf.

[58] 50 U.S.C. § 4565 (2019).

to suspend or block any proposed or pending foreign "mergers, acquisitions, or takeovers" that could result in foreign control of a United States business that would threaten to impair national security.[59]

In November, 2018, CFIUS adopted an interim pilot program that expanded CFIUS's scope and made effective mandatory declarations.[60] Businesses that fall under the scope of CFIUS have to file a declaration to CFIUS if a foreign transaction is expected.[61]

In 2016, China invested $18.7 billion in 107 U.S. tech firms.[62] In April 2019, CFIUS demanded that Chinese owners of Grindr,[63] a dating app geared toward LGBTQ+ community members, give up control of the company after the Chinese owners had strategically bought out the American company.[64] Since Grindr keeps a lot of user data and tracks its user's movements, many U.S. officials and government contractors' identities could be compromised.[65] CFIUS's decision to stop this transaction demonstrates that CFIUS is expanding its view of national

---

[59] Jackson, *supra* note 57, at 7.

[60] *Fact Sheet: Interim Regulations for FIRRMA Pilot Program*, DEPT. OF TREAS. (Oct. 10, 2018), https://home.treasury.gov/system/files/206/Fact-Sheet-FIRRMA-Pilot-Program.pdf.

[61] *Id*.

[62] Sarah Bauerle Danzman & Geoffrey Gertz, *Why is the U.S. forcing a Chinese company to sell the gay dating app Grindr?*, WASH. POST (Apr. 3, 2019), https://www.washingtonpost.com/politics/2019/04/03/why-is-us-is-forcing-chinese-company-sell-gay-dating-app-grindr/?utm_term=.2f816bf80702.

[63] GRINDR, https://www.grindr.com/ (last visited Aug. 16, 2019).

[64] Danzman, *supra* note 62.

[65] *Id*.

security.[66] Since 2018, after CFIUS scrutiny increased, Chinese investments decreased to $2.2 billion for 80 deals.[67] The question remains whether a blanket limit on Chinese investments is a national security interest or harmful to the U.S. economy.

The interplay between export control and CFIUS is significant because it increases the opportunities for regulation of emerging technologies in the interest of national security. However, even under CFIUS, the specified goals of national security are elusive. Importantly, FIRRMA, which bolstered and expanded CFIUS's jurisdiction and functions, and the legislation requiring an ANPRM for emerging and foundational technologies were published in the same statute, the National Defense Authorization Act.[68] This statute widely concerns for national security in a time where technology is rapidly developing. Additionally, identifying "emerging technologies" under the recent ANPRM will become the "critical technologies" for CFIUS purposes.[69] Meaning, using the term critical technologies in lieu of emerging technologies, CFIUS will also regulate investments in technologies that this ANPRM finds necessary to regulate. Therefore, the current ANPRM for identifying emerging technologies has a huge potential impact on regulation and the public's understanding of national security.

---

[66] *Id*.

[67] *Id*.

[68] 50 U.S.C. §§ 4565, 4817.

[69] Kay C. Georgi & Marwa M. Hassoun, *Action Alert: BIS Publishes List of Emerging Technologies That It Is Considering Subjecting to Unilateral US Export Control. Your Company May Need to File Comments by December 19, 2018!*, ARENT FOX: PERSPECTIVES (Nov. 21, 2018), https://www.arentfox.com/perspectives/alerts/commerce-department-requests-public-comments-emerging-technologies-export.

PART TWO: EXPLAINING THE EAR

A. What is the Export Administration Regulations (EAR)?

The Department of Commerce's Bureau of Industry and Security (BIS) regulates the export of certain commercial products and technologies under the EAR.[70] Specifically, a small percentage of exports and reexports require a license.[71] Exports that are regulated are listed in mainly two ways: through the Commerce Control List (CCL) and through the Entity List, which details the prohibition or restriction of commerce to certain countries and end users.[72] The difference between these two ways is that through the CCL, the EAR regulates specific categories of products that require a license for its export.[73] Through the Entity List, the EAR regulates specific "Persons and Entities" from participating in commerce.[74] The Entity List includes details of countries and end-users that have embargoes and foreign trade policy restrictions.[75]

B. EAR Controls

The EAR specifies five facts that determine what obligations apply under the EAR: 1)

---

[70] *Overview of U.S. Export Laws*, U. OF KAN., https://export-compliance.ku.edu/overview-us-export-laws (last visited Aug. 2, 2019).

[71] 15 C.F.R. §730.7 (2017).

[72] *Id*.

[73] *Id*. at §774 (2018).

[74] *Id.* at Supp. 4 to §744 (2019).

[75] *Id*.

"What is it?"[76] This entails the classification of the item and whether it is placed on the CCL. If the item is on the CCL, then it may require a license.[77] 2) "Where is it going?"[78] The ultimate country of destination for an export or reexport may also determine whether a license is required for export.[79] 3) "Who will receive it?"[80] This requirement clarifies the "end-user" of the item.[81] Some types of end-users cannot receive exports.[82] 4) "What will they do with it?"[83] This question asks what the "end-use" of the item will be.[84] Exports cannot be sent for certain end-uses.[85] And 5) "What else do they do?"[86] Certain types of conduct, such as "contracting, financing, and freight forwarding" in support of a "proliferation project" may prevent the export

[76] *Id*. at §732.1(b) (2017).

[77] *Id*.

[78] *Id*.

[79] *Id*.

[80] *Id*.

[81] *Id*.

[82] *Id*.

[83] *Id*.

[84] *Id*.

[85] *Id*.

[86] *Id*.

to someone.[87] Additionally, an exporter must check to see if the item requires a license under one of ten general prohibitions subject to the EAR.[88]

C. Types of Products Currently Controlled

The EAR's broad categorization of exports reflects its mindfulness of national security concerns. Generally, types of exports are controlled under the CCL, which is divided into ten categories: "0-Nuclear Materials, Facilities and Equipment and Miscellaneous; 1-Materials, Chemicals, 'Microorganisms,' and Toxins; 2-Materials Processing; 3-Electronics; 4-Computers; 5-Telecommunications and Information Security; 6-Lasers and Sensors; 7-Navigation and Avionics; 8-Marine; 9-Aerospace and Propulsion."[89] These categories are further divided and arranged by groups: "A: Equipment, Assemblies and Components; B-Test, Inspection and Production Equipment; C-Materials; D-Software; E-Technology."[90] What is important about these categories is realizing the EAR's vague categorizations. Many of these categories may even already cover emerging technologies in some way, thereby further highlighting existing inefficiencies in regulations.[91] Additionally, technologies under one category may possibly fall

[87] *Id*.

[88] *See id*. at §732.1(d) (listing a brief description of the ten general prohibitions, *inter alia*, the exports or reexports of controlled items to listed countries; exports and reexports from abroad of the foreign-produced direct product of U.S. technology and software; export or reexport to prohibited end-users and end-uses; export or reexport to embargoed destinations).

[89] *Id.* at §738.2(a) (2018).

[90] *Id.* at §738.2(b) (2018).

[91] *See id*.

under another category.[92] Given these existing categorizations, it is difficult to imagine how emerging technologies would be separately categorized.

The CCL also provides a designated acronym that identifies a "Reason for Control."[93] Although a control can designate more than one reason, it seems as though "National Security" as a reason is a "catch-all" category.[94] In the context of identifying emerging technologies, the question is whether the "interest of national security" will be the same reasons already outlined in the CCL?[95]

D. The Export Control Classification Number (ECCN)

---

[92] *See id*.

[93] *See id.* at §738.2 (d)(2)(ii)(A) (listing fourteen different reasons that exports can be controlled and its acronym. AT: Anti-terrorism; CB: Chemical & Biological Weapons; CC: Crime Control; CW: Chemical Weapons Convention; EI: Encryption Items; FC: Firearms Convention; MT: Missile Technology; NS: National Security; NP: Nuclear Nonproliferation; RS: Regional Stability; SS: Short Supply; UN: United Nations Embargo; SI: Significant Items; SL: Surreptitious Listening). Several of these specifications seem to objectively imply a national security issue, such as anti-terrorism. However, the inclusion of national security seems vague, compared to most of the other specifications.

[94] *Cf. id*. (listing fourteen specific categories, of which National Security is not necessarily the most specific); *see supra* note 93 and accompanying text.

[95] *See* 15 C.F.R. §742.4 (2018) ("It is the policy of the United States to restrict the export and reexport of items that would make a significant contribution to the military potential of any other country or combination of countries that would prove detrimental to the national security of the United States").

Businesses have the opportunity to request classifications from the BIS and obtain licenses for exports.[96] In the request, the business describes the product that it wishes to export, according to the form requirements, and submits that form to the BIS.[97] The BIS then provides an Export Control Classification Number (ECCN) if applicable.[98] The ECCN specifies the type of export.[99] Each ECCN is either in the CCL, Supplement No. 1 to Part 774 of the EAR, and if not described by an ECCN, then it is an EAR99 item.[100] Depending on the ECCN, certain exports to CCL-specified countries and end-users are controlled, which means a license could be required if a business wants to export a product with an ECCN that falls under the CCL.[101] This classification process is supposed to be a streamlined way for businesses to obtain licenses from the BIS.

Depending on the ECCN, exceptions to getting licenses may also apply.[102] Exports outlined in the License Exception ENC,[103] do not require businesses to obtain a license. However, certain encryption technologies or digital forensics require annual or semi-annual

[96] 15 C.F.R. §748.1 (2017).

[97] *Id*. at §748.3 (2016).

[98] *Id*.

[99] *Id*.

[100] *Id*.

[101] *Id*.

[102] *Id*. at §740.17 (2019).

[103] *Id*.

reports.[104] This is a creative way for the BIS to garner information on technologies that could be used to help form and administer national security policies.

E. EAR Violations

The EAR provides detailed specifications of the types of violations and sanctions under the EAR.[105] Although violations of the EAR seldom go to court, some cases have managed to make it through. A thorough analysis of EAR violations and court opinions is outside the scope of this Comment. However, to illustrate what EAR violations look like in the judicial process, the following is a brief mention of three cases: In *United States v. Ihsan Elashyi*,[106] the defendants shipped exports to Libya through Malta. They were charged under the Export Administration Act (EAA), which authorized the "Secretary of Commerce to issue regulations prohibiting or curtailing exports in order to protect or further the national security, foreign policy, or short-supply interests of the United States."[107] In *United States v. Zhen Zhou Wu*,[108] the defendant exported electronic converters controlled under the CCL to China.[109] In *United States v. Geisser*,[110] the defendant exported F-14 aircraft tires to Iran.[111] Interestingly, the

[104] *Id*.

[105] *Id*. at §764.2 (2013).

[106] 554 F.3d 480, 489 (5th Cir. 2008).

[107] *Id*. at 492.

[108] 711 F.3d 1, 8 (1st Cir. 2013).

[109] *Id*. at 21–25.

[110] 731 F. Supp. 93, 94–96 (E.D.N.Y. 1990).

[111] *Id*. at 96.

court in this situation decided whether the classification of an ECCN covered the commodity being exported.[112]

However, most violations do not reach court. When serious violations occur, the BIS can take measures to include a violating business onto an export controlled Entity List.[113] For example, in March 2016, the BIS placed ZTE Corp., a prominent Chinese technology corporation, on its Entity List—barring U.S. exporters from selling to the company.[114] ZTE violated sanctions on Iran.[115] The BIS imposed a penalty of $1.1 billion dollars in 2017 before removing ZTE from the entity list.[116] ZTE then violated the settlement terms, received a full export ban, and racked up an additional $1.4 billion penalty.[117]

1) 5G and Huawei

Recently, news headlines have featured the Trump Administration's ban on Huawei.[118]

---

[112] *Id*. at 96–97.

[113] *See supra* PART TWO (A).

[114] Alex Lawson, *History Gives No Clues to Trump-Huawei Endgame*, LAW360 (May 24, 2019), https://www-law360-com.proxy.wcl.american.edu/articles/1163090/history-gives-no-clues-to-trump-huawei-endgame.

[115] *Id*.

[116] *Id*.

[117] *Id*.

[118] *See, e.g.*, Jeanne Whalen, Reed Albergotti & David J. Lynch, *U.S. tech firms push Trump to allow sales to Huawei, set up White House meeting next week*, WASH. POST (July 19, 2019), https://www.washingtonpost.com/business/2019/07/19/us-tech-companies-push-trump-allow-

In January, the Bureau of Industry and Security (BIS) placed Huawei Technologies Ltd., which is the biggest maker of network equipment for phone companies, on its entity list.[119] American officials accused Huawei of facilitating Chinese spying, an allegation Huawei has denied.[120] Huawei is one of the biggest buyers of U.S. suppliers of chips and other technologies.[121] The White House issued a temporary reprieve, allowing sales with Huawei to continue for 90 days; that period has expired.[122] President Trump's decision to ban Huawei sparked national security debates.[123]

---

some-sales-huawei/?utm_term=.9f355286e0d8 (reporting U.S. tech companies attempts to receive licenses to deal with Huawei); *see also* 15 C.F.R. § 744 (2019).

[119] Dake Kang, *Huawei calls on US to lift export restrictions*, WASH. POST (July 12, 2019), https://www.washingtonpost.com/newssearch/?datefilter=All%20Since%202005&query=huawei&sort=Relevance&utm_term=.677048c37472.

[120] Maggie Millier, *Blackburn says China building 'spy network' through Huawei technology*, THE HILL (July 8, 2019), https://thehill.com/policy/cybersecurity/452060-blackburn-says-china-building-spy-network-through-huawei-technology; Kang, *supra* note 119.

[121] Kang, *supra* note 119.

[122] Jeanne Whalen, Reed Albergotti & David J. Lynch, *U.S. tech firms push Trump to allow sales to Huawei, set up White House meeting next week*, WASH. POST (July 19, 2019), https://www.washingtonpost.com/business/2019/07/19/us-tech-companies-push-trump-allow-some-sales-huawei/?utm_term=.9f355286e0d8.

[123] *See* Sean Kean, *Huawei ban: Full timeline on how and why its phones are under fire*, CNET (Aug. 16, 2019 3:05 AM), https://www.cnet.com/news/huawei-ban-full-timeline-on-how-and-why-its-phones-are-under-fire/ (presenting a timeline of President Trump's Huawei ban);

This ban, which is seemingly in the interest of national security, has profound economic interests as well.[124] Despite Huawei allegedly dealing with Iran,[125] facilitating spying for

---

Compare Reed Albergotti, *Huawei ban threatens U.S. national security, tech companies warn Trump administration*, WASH. POST (June 7, 2019), https://www.washingtonpost.com/technology/2019/06/07/huawei-ban-threatens-us-national-security-tech-companies-warn-trump-administration/ (reporting that U.S. technology companies informed the Commerce Department that the Huawei ban could severely damage the ability to develop "new technological innovations, including those needed by the U.S. military"), *and* Bloomberg, *Google warns Washington that Huawei trade ban risks compromising US security: report*, S. CHINA MORNING POST (June 7, 2019, 6:55 PM), https://www.scmp.com/tech/gear/article/3013599/google-warns-washington-huawei-trade-ban-risks-compromising-us-security (reporting that Google warned Washington that Huawei could make its own modified version of Android software because Google cannot update the Android operating system on Huawei smartphones, making the technology vulnerable to hacking risks), *with* Simon Jenkins, *Google's Huawei ban is good news: tech giants shouldn't always get their way*, GUARDIAN (May 20, 2019), https://www.theguardian.com/commentisfree/2019/may/20/google-huawei-ban-tech-giants-donald-trump-blacklist (insisting that President Trump's actions against Huawei, a company that has too eagerly dominated 5G technology, will have good consequences and is in the interests of openness and freedom. "The last weapon against them may be the most cynical: national security, a stock excuse for bogus authoritarianism. But any reason is better than nothing").

[124] *See* Craig Timberg & Reed Albergotti, *Will U.S. war on Huawei help China end its dependency on Western tech?*, WASH. POST (May 24, 2019),

China,[126] and having secret operations to build North Korea's wireless network,[127] Huawei is the leading company in the development of 5G technology.[128] Banning Huawei effectively put a

---

https://www.washingtonpost.com/technology/2019/05/24/tiny-technology-has-giant-consequences-us-china-trade-war/ ("The U.S. move, based on national security concerns, could have long-term consequences that would not be in U.S. interests, spurring the creation of new competitors in an industry now dominated by Western companies such as Qualcomm, Intel, Arm and others").

[125] Kenneth Rapoza, *Further Investigations Show Ties of China's Huawei To Iran*, FORBES (Jan. 8 2019), https://www.forbes.com/sites/kenrapoza/2019/01/08/further-investigations-show-chinas-huawei-broke-iran-sanctions/#2cf969783d6d.

[126] Maggie Millier, *Blackburn says China building 'spy network' through Huawei technology*, THE HILL (July 8, 2019), https://thehill.com/policy/cybersecurity/452060-blackburn-says-china-building-spy-network-through-huawei-technology.

[127] Ellen Nakashima, Gerry Shih & John Hudson, *Leaked documents reveal Huawei's secret operations to build North Korea's wireless network*, WASH. POST (July 22, 2019), https://www.washingtonpost.com/world/national-security/leaked-documents-reveal-huaweis-secret-operations-to-build-north-koreas-wireless-network/2019/07/22/583430fe-8d12-11e9-adf3-f70f78c156e8_story.html?utm_term=.3e5670aae9da.

[128] *How 5G technology could be a potential security risk*, CNN (July 23, 2019), https://www.cnn.com/videos/business/2019/07/23/huawei-cell-phone-avlon-reality-check-newday-vpx.cnn/video/playlists/stories-worth-watching/.

significant stop to its capability of releasing its 5G technology.[129] On April 12, 2019, about a month before an Executive Order banned Huawei, President Trump said, "The race to 5G is on and America must win."[130] Huawei's addition to the entity list in the interest of national security, along with President Trump's public statements about winning the race to 5G, is an example of a national security interest that is blurred by an economic impetus.

PART THREE: THE BIS's ATTEMPT TO IDENTIFY EMERGING TECHNOLOGIES

A. Defining Emerging Technologies

The descriptions of products on the Commerce Control List's (CCL), and the process of obtaining an ECCN reflect the United States' interest in protecting national security.[131] The different categories within the CCL also reflect the Export Administration Regulation's (EAR) attempt to keep up with technology.[132] It is important to recognize the interplay between the

---

[129] Todd Haselton, *President Trump announces new 5G initiatives: It's a race 'America must win'*, CNBC (April 12, 2019, 5:42 PM), https://www.cnbc.com/2019/04/12/trump-on-5g-initiatives-a-race-america-must-win.html?&qsearchterm=President%20Trump%20announces%20new%205G%20initiatives:%20It%27s%20a%20race%20%27America%20must%20win.

[130] *Id*.

[131] 15 C.F.R. §748 (2017); *see also supra* note 22.

[132] *See* Daniele Rotolo, Diania Hicks & Ben Martin, *What is an Emerging Technology?*, SCI. POL'Y RES. UNIT (July, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2743186 (discussing the difficulty of defining an emerging technology. "Yet, as an area of study, emerging technologies lacks key foundational elements, namely a consensus on what classifies a

CCL's current broad categories, and this ANPRM's even broader categorization.[133] The ANPRM's approach to simply name broad classifications of technologies, such as artificial intelligence or data analytics technology, may be so broad as to be a hindrance to innovation.[134] The Act lacks a narrowly tailored approach, along with specified applications of technology that pose a risk to national security.[135]

The National Defense Authorization Act's call upon the agencies to create an interagency process for identifying emerging technologies to update the CCL in the interest of national security is not a surprise, but a continued effort in bolstering U.S. national security.[136] The portion within the National Defense Authorization Act that addresses the identification of emerging technologies is commonly called the Export Control Reform Act (ECRA), a statute that allows the regulation of emerging technologies.[137] Along with ECRA, the Foreign Investment Risk Review Modernization Act (FIRRMA)—which gave the Committee on Foreign Investment in the United States (CFIUS) an even more significant role[138]—was also passed as

---

technology as 'emergent' and strong research designs that operationalize central theoretical concepts").

[133] *See supra* PART TWO (C).

[134] *See supra* note 24.

[135] 15 C.F.R. §744.

[136] 50 U.S.C. § 4817 (2019).

[137] 50 U.S.C. §§ 4801–4852 (2018).

[138] *See supra* PART ONE (C).

part of the 2019 National Defense Authorization Act.[139] To reiterate, both ECRA and FIRRMA were passed in the National Defense Authorization Act.[140]

B. Comments submitted to the ANPRM

In response to the ANPRM, businesses and tech companies have made submitted comments public. Businesses have detailed various concerns and suggestions surrounding the identification of emerging technologies.[141] These comments contain many overlapping ideas regarding how to identify and regulate emerging technologies. Analyzing these comments provides a business perspective on the problem of identifying emerging technologies. Although a thorough analysis of these public comments is outside the scope of this Comment, it is particularly valuable to highlight and entertain some of the comments' considerations.

The Semiconductor Industry Association (SIA) expressed concern that export controls should not impede or undermine the U.S. innovation and technology base.[142] SIA asserts that

---

[139] *See supra* PART ONE (C); *see also The Export Control Reform Act and Possible New Controls on Emerging and Foundational Technologies*, AKIN GUMP: INSIGHTS (Sept. 12, 2018) https://www.akingump.com/en/news-insights/the-export-control-reform-act-of-2018-and-possible-new-controls.html.

[140] 50 U.S.C. § 4817 (2019).

[141] *See, e.g.*, *infra* note 142.

[142] *Comments of the Semiconductor Industry Association on Advanced Notice of Proposed Rulemaking regarding Review of Controls for Certain Emerging Technologies*, SIA (Jan. 10, 2019), https://www.semiconductors.org/wp-content/uploads/2019/01/BIS-ANPRM-on-emerging-technology-jan-10.pdf. The Semiconductor Industry Association (SIA) is a trade association representing the semiconductor industry in the United States. The global market is

maintaining a strong "semiconductor research, design, manufacturing and supplier base is, in itself, a national security issue . . ."[143] Additionally, SIA emphasizes that proposed rules should be in accordance with the standards already set forth in ECRA, which states that unilateral controls should be rare and be used as a response to specific emergency situations essential to our national security.[144]

Business Roundtable's comment addresses the ANPRM with particular attention to ECRA's policy statement, focusing on four primary goals:[145] to adopt narrow a approach, to

---

concentrated in a few major countries; the U.S. holds 50 percent of the global market share. *See id*.

[143] *Id*.; *see also* COUNCIL OF ADVISORS ON SCI. & TECH., EXEC. OFFICE OF THE PRESIDENT, ENSURING LONG-TERM U.S. LEADERSHIP IN SEMICONDUCTORS (Jan. 2017), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_ensuring_long-term_us_leadership_in_semiconductors.pdf ("Cutting-edge semiconductor technology is also critical to defense systems and U.S. military strength, and the pervasiveness of semiconductors makes their integrity important to mitigating cybersecurity risk").

[144] SIA *supra* note 142.

[145] *Business Roundtable Comments on the Advance Notice of Proposed Rulemaking (ANPRM) regarding the Review of Controls for Certain Emerging Technologies*, BUS. ROUNDTABLE (Jan. 12 2019), https://www.businessroundtable.org/business-roundtable-comments-on-the-advance-notice-of-proposed-rulemaking-anprm-regarding-the-review-of-controls-for-certain-emerging-technologies. The Business Roundtable is an association of chief executive officers. The members of the Business Roundtable together employ more than 15 million people and have

avoid unilateral controls, to coordinate with "allies and other countries," and to consistently and closely consult industries throughout the rulemaking and implementation process.[146]

Along with suggesting that controls on emerging technologies should be narrow and should avoid hindering innovation, IBM's comment suggests several policy questions to help identify an emerging technology:[147] Is the technology really a new and distinctly novel technology?[148] Is the technology growing and evolving?[149] Is the technology widely available, and will controls actually help prevent access to the technology?[150] Do only a select few have the capability to further develop the technology?[151] Is it challenging to reverse engineer the technology, given the state of knowledge?[152] Although these questions are vast, they reaffirm

---

more than $7 trillion in annual revenues. *See id*; *see also About Us*, BUS. ROUNDTABLE, https://www.businessroundtable.org/about-us (last visited Aug. 2, 2019).

[146] BUS. ROUNDTABLE, *supra* note 145.

[147] *IBM Comments to U.S. Department of Commerce on Export Controls for Emerging Technologies*, IBM: THINK POLICY (Jan. 10, 2019), https://www.ibm.com/blogs/policy/technology-export-control/. IBM is a leading business in innovation and technology. It offers many brands and services that offer AI technology, cloud technology, cyber-security innovations, and various consumer products. *See id*; *see also About IBM*, IBM, https://www.ibm.com/ibm/us/en/?lnk=fab (last visited Aug. 2, 2019).

[148] IBM: THINK POLICY, *supra* note 147.

[149] *Id*.

[150] *Id*.

[151] *Id*.

[152] *Id*.

the difficulty in identifying an emerging technology.[153] IBM believes that the fourteen categories established in the ANPRM are exceptionally broad.[154] "A large majority of the list is merely a combination of mature technologies used jointly with commercial and open source software from around the world."[155]

C. Addressing National Security

The ANPRM's call to identify emerging technologies in the interest of national security is not surprising; however, it is inadequate because it fails to provide information of what national security means.[156] The Department of Homeland Security identified steps for the advancement of emerging technologies and national security during its 2018 Analytic Exchange Program.[157] Although these steps offer important footsteps toward business and government

---

[153] *Id*.

[154] *Id*.

[155] *Id*. For example, "Certain forms of artificial intelligence (AI) and machine learning are widely available technologies that have been incorporated into numerous commercial products for decades. . . . These products perform speech recognition and natural language processing in an open domain environment. AI building blocks, such as these, have been taught in academic institutions for decades making them – at a high level – poor candidates for consideration as an 'emerging technology.'" *Id*.

[156] 50 U.S.C. § 4817 (2019).

[157] *See* DEPT. OF HOMELAND SECURITY, EMERGING TECHNOLOGY AND NATIONAL SECURITY 1, 3–4 (July 26, 2018), https://www.dhs.gov/sites/default/files/publications/2018_AEP_Emerging_Technology_and_National_Security.pdf (suggesting the need to "incentivize investors and corporations to consider

collaboration, the steps lack collaboration with businesses specifically in identifying national security objectives. Instead, it relies on promising a fostering environment for the development of innovation, but essentially asks for a stream of information on emerging technologies.[158] Doing so excludes businesses from affecting what national security means, and therefore, effective emerging technology regulation.

PART FOUR: RECOMMENDATIONS

A. Conduct a New Rulemaking

Concerns for national security, especially in the context of technology, are not new. However, recently, discussions of bolstering national security have happened in the context of it being developed in conjunction with the development of emerging technologies.[159] Additionally, the ANPRM did not separately analyze national security from a business's perspective. Because of this miniscule jump of understanding, or rather an assumption based on an understanding of the meaning of national security, it seems that the ANPRM and other governmental policy discussions revolve around the protection of national security in spite of the development emerging technologies.[160] Businesses may feel an inherent lack of need to comply with

---

national security," to address "competitive threats" and "share national security concerns," to form "strategic public-private partnerships" with an effort to allocate capital to support national security, and to ensure that the U.S. "continuously maintains a competitive advantage on global, economic, technological, and geopolitical stages").

[158] *Id*.

[159] *See supra* PART THREE (B), (C).

[160] *See Comments of the Semiconductor Industry Association on Advanced Notice of Proposed Rulemaking regarding Review of Controls for Certain Emerging Technologies*, SIA 1, 2–4 (Jan.

regulations that are found upon such a loose term, especially if regulation procedures would hinder innovation.[161]

The ANPRM vaguely asked for comment on how to identify emerging technologies that are important to national security.[162] While the BIS should have initially provided a list of national security concerns with examples of technologies that could impair U.S. national security, instead the phrase national security is left to speculation and imagination.[163] Therefore,

---

10, 2019), https://www.semiconductors.org/wp-content/uploads/2019/01/BIS-ANPRM-on-emerging-technology-jan-10.pdf (suggesting that the ANPRM should justify how each identified emerging technology is essential to U.S. national security, demonstrating with specificity why a unilateral control for an emerging technology is necessary).

[161] *See Advancing an Innovation Agenda for America*, BUS. ROUNDTABLE, https://www.businessroundtable.org/advancing-an-innovation-agenda-for-america (last visited on Aug. 18, 2019) (quoting JPMorgan Chase CEO Jamie Dimon, chairman of Business Rountable, "Securing a prosperous future in the United States depends on business and government working together to protect networks, safeguard data and meeting the sophistication and relentlessness of our adversaries").

[162] 15 C.F.R. §744 (2019).

[163] For example, it is hard for an objective observer to discern the controls on Huawei and other technologies as anything but an impetus to control trade policies or gain a market advantage; following that perspective, a technology may fall under the need for regulation, even though it may not necessarily need regulation. *See supra* PART TWO (E)(1), note 129 and accompanying text; *but see supra 123*. Because of this lack of clarity in what national security concerns are, businesses and exporters may not be able to identify technologies that would perhaps raise

the Commerce Department should conduct another ANPRM and seek comment on what businesses think how national security concerns arise in its products and exports.

The Bureau of Industry and Security (BIS)'s ANPRM also is fundamentally similar to the above discussion of the Department of Homeland Security's steps. The ANPRM does not address specific national security threats that are the reason for the ANPRM. Rather, it generally uses the term national security, almost as a "catch-all" phrase to force regulation of technologies that are unknown to the BIS.[164]

---

national security concerns. *See IBM Comments to U.S. Department of Commerce on Export Controls for Emerging Technologies*, IBM (Jan. 10, 2019), https://www.ibm.com/blogs/policy/technology-export-control/ (suggesting that certain technologies that would fall under the fourteen broad categories listed in the ANPRM should not be contenders of being emerging technologies for regulation).

[164] The ANPRM notes three general considerations: (i) the development of emerging and foundational technologies in foreign countries; (ii) the effect export controls imposed pursuant to this section may have on the development of such technologies in the United States; and (iii) the effectiveness of export controls imposed pursuant to this section on limiting the proliferation of emerging and foundational technologies to foreign countries[.] 50 U.S.C. § 4817 (a)(2)(B) (2019). An interpretation of these considerations makes it seem as though the government has made the policy of remaining market leaders in innovation as its interest of national security. *See supra* note 118. Further, the ANPRM fails to address a process ensuring a clear reason for the regulation of new emerging technologies. *See* Review of Controls for Certain Emerging Technologies, 83 Fed. Reg. 58,201 (Nov. 19, 2018) (to be codified at 15 C.F.R. § 744) (2018).

In light of demonstrated concerns over the meaning of national security and its implications for businesses and innovation, the Commerce Department should undergo another ANPRM, and involve businesses and exporters to define national security in the context of emerging technologies. Counterpoints for such a suggestion is that allowing businesses to be aware of national security concerns undermines national security.[165] Lots of information would be classified; allowing certain business owners to become privy to such information is not practical and could undermine national security.[166]

A comprehensive analysis of national security as a policy is outside the scope of this comment; however, another rulemaking phase to clarify national security would help businesses in the identification and regulation of emerging technologies.[167] The BIS could explain national

---

[165] *See* Nathan Busch & Austen Givens, *Public-Private Partnerships in Homeland Security: Opportunities and Challenges*, HOMELAND SECURITY AFFAIRS (2012), https://www.hsaj.org/articles/233#ref11 (discussing many challenges that face the "privatization of national security functions," such as the increasing need for transparency, while posing the question whether private businesses should be held to the same ethical standards as the public sector?).

[166] *See id*. ("Public-private partnerships can also create proprietary and legal risks for companies. What assurances, for example, do firms have that [the] government will protect proprietary or sensitive information? The WikiLeaks scandal underlines that classified national security information can quickly enter the public domain, damaging the national interest").

[167] *See, e.g.*, *Comments of the Semiconductor Industry Association on Advanced Notice of Proposed Rulemaking regarding Review of Controls for Certain Emerging Technologies*, SIA 1, 5–6 (Jan. 10, 2019), https://www.semiconductors.org/wp-content/uploads/2019/01/BIS-

security in three ways, which are consistent with the policies of the Export Control Reform Act[168]: First, the BIS should define national security from a business perspective as being a consideration of market leadership and military technological advances. Market leadership is important because the U.S. can stay ahead of other countries or bad actors that may use an emerging technology for an unknown future use.[169] If the U.S. does not understand or even have the technology, then national security may be compromised.[170] The BIS could explain this in the context of 5G technology.[171] Further, military technological advances are a national security concern that has long been recognized.[172] However, the BIS could provide examples of particular military uses of technology, such as unmanned aircrafts,[173] which could serve as

---

ANPRM-on-emerging-technology-jan-10.pdf (asserting the need for clarification on what essential national security concerns will implicate emerging technologies).

[168] 50 U.S.C. §§ 4801–4852 (2018).

[169] *See* THE WHITE HOUSE, NATIONAL SECURITY STRATEGY OF THE UNITES STATES OF AMERICA 1, 21 (Dec. 2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf ("Private industry owns many of the technologies that the government relies upon for critical national security missions. . . . The United States must regain the element of surprise and field new technologies at the pace of modern industry").

[170] *See id*.

[171] *See supra* note 93.

[172] *See* NATIONAL SECURITY STRATEGY OF THE UNITES STATES OF AMERICA, *supra* note 169.

[173] *See* Yang Yi, *China-made solar-powered unmanned aircraft makes maiden flight*, XINHUA NET (June 30, 2019), http://www.xinhuanet.com/english/2019-07/30/c_138270560.htm (describing a Chinese company that made a solar-powered unmanned aircraft, which will be used

examples of technologies that foreign militaries are using. U.S. corporations could then identify technologies that may raise similar concerns.

Second, the BIS should declare technologies that could allow or facilitate cyberattacks as a national security concern.[174] Cyberattacks have persistently compromised national security. Already this year, countries and bad actors have carried out countless cyberattacks against U.S. companies and the U.S. government.[175] Iran developed a network of websites and accounts that spread false information about the U.S,[176] the Chinese intelligence service used NSA hacking tools to gather sensitive information,[177] and an unknown, possibly state-sponsored hacker tried to spear-phish three U.S. utility companies to gain important data.[178] It seems that cyberattacks try to either gain sensitive data, or disrupt digital infrastructures. If the BIS were to declare

---

for disaster relief, reconnaissance, and communication; the company said it would also expand the aircraft's application by making it work with 5G technology).

[174] *See supra* PART TWO.

[175] Lily Hay Newman, *The Biggest Cybersecurity Crises of 2019 So Far*, WIRED (July 5, 2019), https://www.wired.com/story/biggest-cybersecurity-crises-2019-so-far/.

[176] *Significant Cyber Incidents Since 2006*, CTR. FOR STRATEGIC & INT'L STUD., https://csis-prod.s3.amazonaws.com/s3fs-public/190523_Significant_Cyber_Events_List.pdf (last visited Aug. 2, 2019).

[177] *Id*.

[178] Sean Lyngaas, *A potentially state-sponsored hacking campaign tried to phish U.S. utilities in July, researchers say*, CYBERSCOOP (Aug. 1, 2019), https://www.cyberscoop.com/apt-10-utilities-phishing-proofpoint/.

technologies that could possibly facilitate cyberattacks as a blanket national security concern, then companies could better identify related emerging technologies.

Third, the Commerce Department should elucidate which foreign entities, especially Chinese corporations, will possibly pose a national security threat, using the example of 5G technology and the placement of Huawei on the entity list.[179] The main counterpoint to this is that businesses cannot be expected to know that espionage, such as the case with Huawei,[180] is likely. However, such an area is precisely where the BIS can provide a list of entities, or even specific corporations, which pose as possible security threats, relying on threats that have been recently exposed. Exporters could use this list to then identify possible emerging technologies that the Chinese, or any malicious entity, may have access to through their dealings.

Additionally, similar to CFIUS, the Commerce Department can undertake a pilot program to determine the scope of emerging technologies that would implicate national security concerns.[181] Last year, CFIUS began a pilot program that expanded its jurisdiction and immediately made effective certain mandatory requirements.[182] Because the program required certain businesses to file declarations, CFIUS often did not give clear replies to filings,

---

[179] *See supra* note 114–129.

[180] *Id*.

[181] *See supra* PART ONE (C).

[182] *See* Determination and Temporary Provisions Pertaining to a Pilot Program To Review Certain Transactions Involving Foreign Persons and Critical Technologies, 83 Fed. Reg. 51,322 (Nov. 10, 2018) (to be codified at 31 C.F.R. pt. 801).

commonly called a "shrug."[183] The Commerce Department can borrow the elements of mandatory filings and initiate a pilot program that would require certain exporters to file declarations and provide information about their technologies.

B. Create a New Committee

The ANPRM calls for an interagency process, considering both public and classified information, as well as information from the Emerging Technology Technical Advisory Committee and CFIUS.[184] This likely means that, since multiple committees are involved, information must be consolidated and competing policies must be sorted out. Similar to the inefficiencies created by exports being regulated by multiple agencies, having a multi-committee, interagency process to identify emerging technologies will make inefficiencies and complications inevitable.[185] To solve these issues, the Commerce Department should create a single agency that specifically handles the tracking of developing technologies.

---

[183] *See* Doreen M. Edelman & Louis K. Rothberg, *Key Takeaways From Six Months Into New Mandatory CFIUS Pilot Program*, LOWENSTEIN SANDLER: CLIENT ALERT (June 17, 2019), https://www.lowenstein.com/news-insights/client-alerts/key-takeaways-from-six-months-into-new-mandatory-cfius-pilot-program-global-trade-policy; *see also* Stephen Heifetz & Joshua Gruenspecht, *CFIUS 2.0 Roundup: The Pilot Program, The Shoulder Shrug*, LAW360 (March 29, 2019, 4:20 PM), https://www.law360.com/articles/1144251/cfius-2-0-roundup-the-pilot-program-the-shoulder-shrug (commenting that there has been little guidance and little enforcement on how to interpret the pilot program rules).

[184] 15 C.F.R. § 744 (2019).

[185] *See supra* PART ONE (B).

Consolidating the process of identifying emerging technologies should be similar to the Obama Administration's attempt to consolidate the multiple export agencies.[186] The Obama Administration attempted and sought to create a single control list, a single licensing agency, a unified information technology system, and a single enforcement agency.[187] It accomplished this by moving items under the jurisdiction of another agency into the jurisdiction of the Export Administration Regulations (EAR).[188] The Trump Administration is also continuing to consolidate agencies. Recently, the BIS issued a proposed rule that would consolidate several items on the United States Munitions List (USML), which is a control list of exports intended for military use under the State Department, with the EAR's CCL.[189] The consolidated items would receive a new ECCN series, and its regulation would be subject to the EAR's jurisdiction. Similar to this consolidation of agency functions, a single committee should develop and gather

---

[186] *About Export Control Reform*, EXPORT.GOV, http://2016.export.gov/ecr/ (last visited Aug. 2, 2019); *see supra* PART ONE (B).

[187] *See* James E. III Bartlett & Jonathan C. Poling, *Defending the Higher Walls - The Effects of U.S. Export Control Reform on Export Enforcement*, 14 SANTA CLARA J. INT'L L. 1, 2 (2016) (discussing how export control enforcement should continue during "Export Reform" and the consolidation of functions).

[188] *Id*.

[189] Control of Firearms, Guns, Ammunition and Related Articles the President Determines No Longer Warrant Control Under the United States Munitions List (USML), 83 Fed. Reg. 24,166 (May 24, 2018) (to be codified at 15 C.F.R. pt. 736, 740, 742, 743, 744, 746, 748, 758, 762, 772, 774).

information about emerging technologies. That single committee would then provide the information to the various controlling agencies, and especially to the Commerce Department.

Admittedly, an Office of Science and Technology Policy (OSTP) already exists.[190] From the description of this agency, the OSTP is responsible for providing "the President and others within the Executive Office of the President with advice on the scientific, engineering, and technological aspects of the economy, national security, homeland security, health, foreign relations, the environment, and the technological recovery and use of resources, among other topics."[191] However, despite the existence of an agency whose function seemingly relates directly to the identification of emerging technologies in the interest of national security, the ANPRM calls upon an interagency process, specifying the Emerging Technology Technical Advisory Committee and CFIUS.[192] At the confluence of these agencies lies the confusion and complications.[193] Learning from the past attempts of consolidating the entire system of export

---

[190] Office of Science and Technology Policy, THE WHITE HOUSE, https://www.whitehouse.gov/ostp/ (last visited Aug. 2, 2019).

[191] *Id*.

[192] 15 C.F.R. § 744 (2019)

[193] *Compare Emerging Technology Technical Advisory Committee*, DEPT. OF COM., https://tac.bis.doc.gov/index.php/ettac-home (last visited Sept. 20, 2019) (describing the function of the emerging technology technical advisory committee as identifying emerging technologies that implicate national security concerns for the next five to ten years), *and Technical Advisory Committees (TAC)*, DEPT. OF COM., https://tac.bis.doc.gov/index.php (last visited on Sept. 20, 2019) (describing the general functions of a technical advisory committee as industry members "appointed by the Secretary of Commerce" that represent the "concerns of the exporting

controls, a single agency with hired technology experts and scientists would streamline the identification of emerging technologies.[194] This comment recommends that such a function should be delegated to the already existing OSTP, or to a newly created committee.

---

community"), *with The Committee on Foreign Investment in the United States (CFIUS)*, DEPT. OF THE TREAS., https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius (last visited on Sept. 20, 2019) (describing CFIUS as an interagency process to review certain foreign investments in the United States, "in order to determine the effect of such transactions on the national security of the United States"), *and supra* PART ONE (C).

[194] *See* James E. III Bartlett & Jonathan C. Poling, *Defending the Higher Walls - The Effects of U.S. Export Control Reform on Export Enforcement*, 14 SANTA CLARA J. INT'L L.1, 4 (2016) (commenting that the Export Reform efforts via the consolidation of controlled items to the CCL has been criticized by some as "deregulation," but reforms have generally "been well received by American industry and its foreign customers, who had long complained that the current system was unnecessarily burdensome") (citing *The Export Administration Act: A Review of Outstanding Policy Considerations: Hearing Before the Subcomm. On Terrorism, Nonproliferation and Trade of the H. Comm. on Foreign Affairs*, 111th Cong. 22 (2009) ("The Focus of export control reforms should be on ensuring that the system protects U.S. national security in the 21st century—not on removing the remaining speed bumps on the export superhighway"); David R. Fitzgerald, *Leaving the Back Door Open: How Export Control Reform's Deregulation May Harm America's Security*, 15 N.C.J.L. & TECH 65, 89 (2014) (former Army Ranger and Afghanistan War veteran criticizing justifications advanced for Export Control Reform); Benjamin Goad, *Export Control Overhaul Sparks National Security Scrap*,

In addition to the creation of a single committee to deal with the continuous identification of emerging technologies, the EAR could require reports from exporters that acquire an Export Control Classification Number (ECCN). Currently, certain exports are allowed an exception from getting a license, but are instead required to file reports.[195] Similarly, the EAR could require exporters that request ECCNs for CCL items that already exist for technologies to submit a report about three things: first, a detailed report about the technology that is being exported and its availability in the foreign market; second, a speculative report about what hindrances in innovation the company would suffer from various degrees of export controls; and third, a report about whether export controls would affect the international proliferation of the technology and

---

THE HILL (Oct. 17, 2013, 12:47 AM), *available at* http://bit.ly/1CQenvT ("In my mind, it's a major deregulation," said Steven Pelak, a former national coordinator for export control enforcement at the Justice Department. Pelak . . . said that effort would make it easier for nations like Iran and China to 'obtain our spare parts.'")); *see* Bartlett, *Defending the Higher Walls - The Effects of U.S. Export Control Reform on Export Enforcement* at note 18 (citing *Export Control Reform: The Agenda Ahead, Hearing Before the H. Comm. of Foreign Affairs*, 113th Cong. 4 (Apr. 24, 2013) (statement of Thomas Kelly, Acting Assistant Sec'y, Bureau of Political-Military Affairs, U.S. Dep't of State) ("But because our current export controls are confusing, time consuming, and many would say overreaching, our allies increasingly seek to design out U.S. parts and services thus avoiding our export controls, and use monitoring that comes with them, in favor of indigenous design. This threatens the viability of our defense industrial base especially in these austere times")).

[195] *See supra* PART TWO (D).

to what degree.[196] The single committee designated for tracking emerging technologies could receive this report, suggesting additions to the CCL as it sees fit.

CONCLUSION

The Department of Commerce must have realistic and clear goals for regulating emerging technologies. The current ANPRM simply stated that the addition of emerging technologies to the Commerce Control List is in the interest of national security, but it did not specify or ask how such an addition would not hinder innovation in the United States,[197] nor did it clarify what national security means. The Commerce Department should issue a separate rulemaking phase to identify what the national security interests are—in the context of emerging technologies—and perhaps create a new committee that works with leading technology companies to continuously identify emerging technologies. These two recommendations, in conjunction with initiating a pilot program and innovative controls that require reporting, would help the government and businesses solve the emerging technologies and national security conundrum.

[196] *See id*; *see also* 50 U.S.C. § 4817 (a)(2)(B) (discussing three considerations that the interagency process should take into account); *see supra* INTRODUCTION.

[197] *See* Review of Controls for Certain Emerging Technologies, 83 Fed. Reg. 58,201 (Nov. 19, 2018) (to be codified at 15 C.F.R. § 744) (2018).