MassPoint PLLC LEGAL AND STRATEGY ADVISORY - <u>Strategic Legal Counsel</u>

Commerce Department Opens Process to Identify "Emerging Technologies" for Export Control, Public Comments Due by December 19

On November 19, the U.S. Department of Commerce, Bureau of Industry and Security ("**Commerce**") published an <u>Advance Notice of</u> <u>Proposed Rulemaking</u> (**ANPRM**) on the "Review of Controls for Certain Emerging Technologies." The ANPRM invites public comment to identify "emerging technologies" that are essential to U.S. national security and therefore potentially subject to export control.

The ANPRM raises diverse legal, regulatory, policy, and commercial issues that cut across sectors and industries. Commerce seeks to advance national security goals without harming the United States' capacity to lead in science, technology, engineering, and manufacturing. The task of identifying emerging technologies will be daunting as relevant emerging technologies and their civilian and military applications are not sufficiently understood or developed.

Commentators should understand the applicable legal and policy framework, the interagency process, the information and constituencies that will inform the process, and the domestic and international context in which the ANPRM has arisen. The remainder of this update discusses the ANPRM's legal and policy framework and salient features, as well as points for parties to consider in formulating comments.

Public comments are due on or before December 19, 2018 and can be transmitted electronically through the Federal eRulemaking Portal or by mail to Commerce (see the ANPRM for specifics).

Law and Policy Context: National Security and Technological Leadership

"The national security of the United States requires that the United States maintain its leadership in the science, technology, engineering, and manufacturing sectors, including in foundational technology that is essential to innovation."¹ This national policy is declared in the Export Control Reform Act of 2018 (**ECRA**), a significant measure that, in tandem with the Foreign Investment Risk Review and Modernization Act (**FIRRMA**), lays the groundwork for strengthened controls of transfers of U.S.-origin technologies whether by exports or commercial or other transactions—deemed Regulatory Update | Nov. 25, 2018

SNAPSHOT

- The Department of Commerce on Nov. 19 invited public comment to identify "emerging technologies" that are essential to national security and potentially subject to export controls.
- Commerce has identified 14 categories of emerging technology for consideration, including Artificial Intelligence, brain-computer interfaces, and quantum information and sensing technology.
- Commerce's action is mandated by the Export Control Reform Act of 2018 that lists "emerging technologies" as critical to national security and requires Commerce to identify them.
- Protecting the United States' technological edge vis-à-vis other nations (*e.g.*, China) is a key objective, as is preserving U.S. military superiority.
- As emerging technologies have multiple known or potential civilian and/or military applications, identifying which technologies or applications should be controlled and for which policy purpose will be difficult.
- Public comments are due on or before December 19, 2018.
- The 30-day comment period is fairly short, perhaps suggesting high priority.

AUTHOR CONTACT

Hdeel Abdelhady Principal habdelhady@masspointpllc.com +1.202.630.2512

This publication is provided for informational purposes only. This publication is not intended, and should not be construed or relied upon, as legal or other professional advice. This publication may be Attorney Advertising under applicable rules of professional conduct.

Copyright $\ensuremath{\mathbb{C}}$ 2018 MassPoint Legal and Strategy Advisory PLLC. All rights reserved.

essential to U.S. national security, which includes maintaining both U.S. military and industrial and innovation superiority vis-à-vis other nations (such as China).²

Toward stated policy ends, ECRA authorizes and mandates the President to control exports of "items subject to the jurisdiction of the United States."³ The President's obligations include establishing an interagency process to identify "emerging and foundational technologies" that are "essential to the national security of the United States," and therefore may require export control.⁴

At the regulatory implementation level, ECRA authorizes the Secretary of Commerce, acting on behalf of the President and within the interagency process, to establish "appropriate controls" of emerging and foundational technologies⁵ deemed through the interagency process to be essential to national security.

In issuing the ANPRM, Commerce took an early and important step in implementing the ECRA-mandated process for controlling exports of emerging and foundational technologies. As discussed in more detail below, the ANPRM seeks public comment to, among other things, identify emerging technologies essential to U.S. national security and lists 14 "representative technology categories," including Artificial Intelligence, "advanced computing technology," and "brain-computer interfaces," for potential designation (the full list is reproduced below).

Regulatory Need to Define Emerging Technologies Essential to National Security; Integration Into EAR

"Emerging and foundational technologies" are a statutory category of "critical technologies" but are not defined by illustration or otherwise.⁶ Critical technology, in turn, includes any technology designated by the President to be essential to the national defense."⁷ Through the regulatory process commenced by the ANPRM, emerging technologies of national security import are to be specifically identified. Accordingly, the ANPRM seeks public comment on, among other matters, "criteria for identifying emerging technologies that are essential to U.S. national security."

When identified and made subject to export controls, emerging technologies will be part of the Export Administration Regulations (**EAR**) governing exports, reexports, and in-country transfers,⁸ and will also be subject to other provisions of ECRA, including certain information disclosures and "defense industrial base" impact assessments to be made in the course of licensing and other export authorizations (discussed briefly below).

What is Not Covered By the ANPRM: CCL Items, Fundamental Research

Before discussing what the ANPRM covers, it is important to note what is excluded from its scope.

(1) Foundational Technologies Will Be Addressed Separately, for Now

• As discussed below, Commerce is not seeking in the ANPRM process to identify "foundational technologies," but nevertheless seeks comment on whether foundational technologies should be treated as a separate "type" of technology going forward. This is discussed further below.

(2) Technology Currently Described in the Commerce Control List Will Not Be Altered

• Existing controls on technology listed in the Commerce Control List (**CCL**) supplement to the EAR will not be altered as a result of the identification and control of emerging technologies. Items currently listed on the CCL will, per the ANPRM, continue to be "addressed through multilateral regimes or interagency reviews."

(3) Fundamental Research Will Not Be Subject to Commerce's Export Controls Jurisdiction, But Non-Export Control Measures May be Restrict Foreign Participation in Fundamental or Other Research

- The ANPRM states that "Commerce does not seek to expand jurisdiction over technologies that are not currently subject to the EAR, such as 'fundamental research' which is generally defined in § 734.8 of the EAR as "basic and applied research in science and engineering, where the resulting information is ordinarily published and shared broadly within the scientific community."⁹
- The exclusion of fundamental research from Commerce's export control jurisdiction is consistent with long-standing U.S. policy, as set forth in President Reagan's National Security Decision Directive No. 189 of September 21, 1985, on "National Policy on Transfer of Scientific, Technical and Engineering Information" (NSDD 189).¹⁰ Under NSDD 189, the mechanism for limiting dissemination of fundamental research is classification.
- While Commerce does not seek at this time to restrict the export of fundamental research, the Trump Administration and others have considered and likely will continue to consider non-export control measures to directly or indirectly prohibit or limit foreign access to or participation in U.S. fundamental research. For example, proposals to restrict foreign student visas, particularly for Chinese STEM students or all Chinese students, have been floated.¹¹
- Further, concerns among some Administration officials, Congress members, and policy influencers about "academic espionage" and "non-traditional collectors" of sensitive information are propelling action to curb or increasingly scrutinize foreign nationals' access to and participation in U.S. technological development in academic and research settings. A recent example is the Department of Justice's "China Initiative" to combat China's "economic espionage" and other "national security threats" through, *inter alia*, the development of an "enforcement strategy concerning non-traditional collectors (*e.g.*, researchers in labs, universities, and the defense industrial base) that are being coopted into transferring technology contrary to U.S. interests."¹²
- It is conceivable that the Trump Administration, with some bipartisan support in Congress and elsewhere, could modify or replace existing policies on fundamental research, including, perhaps, NSDD 189.

Representative Categories of Emerging Technologies for Potential Export Control; Balancing National Security and Innovation Imperatives

Commerce explains in the ANPRM that "controls of exports of technology are a key component of the effort to protect sensitive U.S. technology" and that "many sensitive technologies are listed on the CCL, often consistent with the lists maintained by the multilateral export control regimes of which the United States is a member" (these multilateral regimes have clear national security and military import, pertaining to, *e.g.*, nuclear weapons proliferation, chemical weapons, and missile technology).

Notably, for ANPRM purposes, Commerce explains further that "[c]ertain technologies . . . may not be listed on the CCL or controlled multilaterally because they are emerging technologies. As such, they have not yet been evaluated for their national security impacts." Through the regulatory process, Commerce "seeks to determine whether there are specific emerging technologies" that are essential to national security and can be more broadly controlled without "negatively impacting U.S. leadership in the science, technology, engineering, and manufacturing sectors." Specifically, Commerce wishes to determine through the regulatory process whether there are, from the list of "representative technology categories" below, "specific emerging technologies that are essential to the national security of the United States." The representative list includes technologies that have been identified for action by government entities and officials and policy influencers in various formats, such as in the U.S. National Security Strategy, government reports, and in Congressional hearings.¹³ Some of the listed technologies also are covered in China's "Made in China 2025" strategy, published in 2015, to elevate China's domestic science and technology capabilities, as well as China's Next Generation Artificial Intelligence Development Plan, published in 2017.

"REPRESENTATIVE TECHNOLOGY CATEGORIES"	
Department of Commerce, Bureau of Industry and Security, ANPRM, 83 F.R. 58202 (Nov. 19, 2018)	
 (1) BIOTECHNOLOGY, SUCH AS: (i) Nanobiology; (ii) Synthetic biology; (iii) Genomic and genetic engineering; or (iv) Neurotech. (2) ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING TECHNOLOGY, SUCH AS: (i) Neural networks and deep learning (<i>e.g.</i>, brain modelling, time series prediction, classification); (ii) Evolution and genetic 	 (7) QUANTUM INFORMATION AND SENSING TECHNOLOGY, SUCH AS (i) Quantum computing; (ii) Quantum encryption; or (iii) Quantum sensing. (8) LOGISTICS TECHNOLOGY, SUCH AS: (i) Mobile electric power; (ii) Modeling and simulation; (iii) Total asset visibility; or
(iii) computation (<i>e.g.</i> , genetic algorithms, genetic	(iv) Distribution-based Logistics Systems (DBLS).
 programming); (iv) Reinforcement learning; (v) Computer vision (<i>e.g.</i>, object recognition, image 	 (9) ADDITIVE MANUFACTURING (<i>E.G.</i>, 3D PRINTING); (10) ROBOTICS SUCH AS: (i) Micro-drone and micro-robotic systems;
understanding); (vi) Expert systems (<i>e.g.</i> , decision support systems, teaching systems);	 (ii) Swarming technology; (iii) Self-assembling robots; (iv) Molecular robotics;
(vii) Speech and audio processing (<i>e.g.</i>, speech recognition and production);	(v) Robot compliers; or
(viii) Natural language processing (<i>e.g.</i> , machine translation);	(vi) Smart Dust. (11) BRAIN-COMPUTER INTERFACES, SUCH AS
(ix) Planning (<i>e.g.</i> , scheduling, game playing);	(i) Neural-controlled interfaces;
 (x) Audio and video manipulation technologies (e.g., voice cloning, deepfakes); 	(ii) Mind-machine interfaces;
(xi) AI cloud technologies; or (xii) AI chipsets.	(iii) Direct neural interfaces; or (iv) Brain-machine interfaces.
(3) POSITION, NAVIGATION, AND TIMING (PNT) TECHNOLOGY.	(i) Flight control algorithms; (ii) Propulsion technologies:
(4) MICROPROCESSOR TECHNOLOGY, SUCH AS:	(iii) Thermal protection systems; or
(I) Systems-on-Chip (SoC); or	(iv) Specialized materials (for structures, sensors, etc.).
(I) Stacked Memory on Chip.	(13) ADVANCED MATERIALS, SUCH AS:
(5) ADVANCED COMPUTING TECHNOLOGY, SUCH AS:	(i) Adaptive camouflage;
(i) Memory-centric logic	(ii) Functional textiles (<i>e.g.</i> , advanced fiber and fabric technology); or
(6) DATA ANALYTICS TECHNOLOGY, SUCH AS:	(iii) Biomaterials.
(i) Visualization;	
(ii) Automated analysis algorithms; or	Faceprint and voiceprint
(iii) Context-aware computing	technologies.

Issues Specifically Identified for Public Comment

(1) Whether "Emerging" and "Foundational" Technologies Should Be Treated as "Separate Types" of Technologies

- As stated above, Commerce will undertake a separate process for identifying "foundational technologies." However, the agency is seeking public comment on whether emerging and foundational technologies should be treated as "separate types of technology." Those submitting public comments should consider, to the extent relevant to their interests, how the separate or joined treatment of emerging and foundational technologies might affect their business, R&D and academic activities, operating environments, and compliance obligations.
- If "foundational technology" is defined along the lines of one National Academies of Sciences, Engineering, and Medicine publication definition—that "foundational technologies (more properly, foundational science and technologies) are by definition those that can enable progress and applications in a variety of problem domains"¹⁴—parties in research and development and commercialization pipelines will likely have an interest in proposing that foundational technology be treated separately, and provide compelling explanations as to why. Academic and research institutions and those that represent their interests might consider how the export regulation of foundational technology, whether separately or together with emerging technology, might relate to or indirectly restrict activities in and related to fundamental research.

(2) Additional Matters on Which Specific Comments Are Requested

Commerce is seeking public comment on the below matters, as well as general comments on the subject matter of the ANPRM:

- The "criteria for identifying emerging technologies that are essential to U.S. national security."
- Commerce seeks comments on the following matters enumerated in the ANPRM:
 - 1. How to define emerging technology to assist identification of such technology in the future;
 - criteria to apply to determine whether there are specific technologies within . . . [the general "representative technology 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 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.

Factors That Commerce Must Consider

By law, Commerce is required consider a number of factors in identifying emerging and foundational technologies that are essential to U.S. national security. Per the ANPRM, these factors are:

- 1. The development of emerging and foundational technologies in foreign countries;
- 2. The effect export controls may have on the development of such technologies in the United States; and
- 3. The effectiveness of export controls on limiting the proliferation of emerging and foundational technologies in foreign countries.

In short, Commerce, by considering these factors, is seeking to gauge the potential effectiveness of any new export controls. For example, restricting exports of technologies that are developed overseas at a pace, in quantities, or at quality levels that match the same technologies produced largely or entirely in the United States would be futile, if not harmful to U.S. interests.

Commerce may also wish to collect further information to assess the degree to which foreign entities or countries of concern (*e.g.*, China), are dependent on U.S.-origin technologies to advance strategic technological or military objectives. The <u>case of ZTE</u> is worth keeping in mind here, as the imposition of a U.S. export ban illustrated the seemingly complete dependence of ZTE (and similarly situated entities) on certain U.S.-origin technological goods. Such information, which can cut different ways, is likely to be valuable when assessing export controls for the purpose of maintaining U.S. technological edge (including by limiting other countries' technological development where they are dependent on U.S. technology in some areas).

Context, Considerations in Formulating Comments

The ANPRM's subject matter and scope affects a range of public and private parties with diverse interests in emerging technologies and their regulation. Technology companies and industry groups, academic and research institutions, national security and defense interests, medical and technology ethicists, and policy professionals, among others, will have an interest in being heard.

In formulating comments, parties should bear in mind the relevant legal framework, the context in which it recently came into being, and the policy goals it is intended to advance. Moreover, the international context is relevant, as are dynamics that are unique to the Trump Administration.

(1) Legal Implications

- As indicated above, controls on exports of emerging and foundational technologies will be integrated into the EAR.¹⁵ And, under ECRA, they will apply broadly "without regard to the nature of the underlying transaction or any circumstances pertaining to the activity." Transfers of emerging technologies made, for example, in the context of marketing, inter-company arrangements, joint ventures, joint development agreements, or other collaborations, will be subject to export controls.¹⁶
- Under ECRA, and at a minimum, a license will be required for the export, reexport, or in-country transfer of emerging technologies to "a country subject to an embargo, including an arms embargo, imposed by the United States." At present, this category includes China.
- In some cases, ECRA requires enhanced information disclosures for parties seeking export authorization in connection with a wide range of commercial, semi-commercial, and non-commercial arrangements. Where an application for an export license or other authorization is submitted "by or on behalf of a

joint venture, joint development agreement, or similar collaborative arrangement," Commerce "may require the applicant to identify, in addition to any foreign person participating in the arrangement, any foreign person with significant ownership interest in a foreign person participating in the arrangement." The task of providing such information, if requested, is likely to be complicated by the imprecise definition of "collaborative arrangement" and silence as to what constitutes "significant" ownership. On the other hand, such a disclosure requirement may benefit some U.S. parties by helping to weed out potential partners with opaque ownership or unwillingness to make required disclosures.

Notably, ECRA contains provisions requiring Commerce to consider the impact on the U.S. "defense industrial base" in making export licensing decisions.¹⁷ While such considerations will have applied previously, by regulatory practice, ECRA codifies and makes uniform (to an extent) defense industrial base assessments. Specifically, ECRA requires Commerce's licensing procedure to provide for an assessment of whether a proposed export "would have a significant negative impact on the United States defense industrial base."¹⁸ A "significant negative impact" occurs when the export, for example, would reduce the availability or production of an item in the United States where the item might be acquired by or produced for Department of Defense.¹⁹

(2) Know the Audience: Interagency Context

Public comments will inform not only Commerce, but also the other cabinet departments and agencies that are part of the interagency process. Pursuant to ECRA, the interagency participants are or will be, in addition to the Secretary of Commerce, the Secretaries of Defense, Energy and State, as well as the heads of other federal agencies "as appropriate."²⁰ Commentators should bear in mind the respective expertise and interests of participating departments and agencies when formulating comments.

(3) Know What the Audience Knows: Information Sources to be Considered in the Interagency Process

Parties who submit comments should also keep in mind that, in the process of identifying emerging and foundational technologies essential to national security, the interagency members will consider, in addition to public comments, "public information and classified information as well as information from the Emerging Technology Technical Advisory Committee and the Committee on Foreign Investment in the United States" (CFIUS).²¹

(4) Examples of Public Information, China-Related Reports

- Public information, it should be noted, includes those public U.S. government reports and unclassified portions of reports that address the national security dimensions of emerging and foundational technologies directly or in the context of discussion about, for example, international military and commercial competition.
- Just this year, for example, a number of reports on China's progress and practices in developing and funding cutting-edge technological capabilities, such as in Artificial Intelligence generally and for military applications, have been numerous. As well, a number of government authored publications— such as by the U.S. Trade Representative, the White House Office of Trade and Manufacturing Policy, and the U.S.-China Economic and Security Review Commission--have discussed China's "intellectual property theft," "academic espionage," strategic investments in U.S. technology companies (to America's disadvantage), and collaborations (via joint ventures, corporate sponsorships, or by other means) with U.S. companies and academic institutions to effect transfers of U.S. technological assets to facilitate the further growth of China's technological and industrial base. The views and information communicated in these reports will likely inform or be considered in the interagency process, and, for some interagency participants, will counsel in favor of emerging technologies export controls.

(5) Non-Public Information Available to the Process Through CFIUS

- As the ANPRM indicates, information obtained by CFIUS in the course of its national security reviews of proposed foreign investments and other transactions in the United States, particularly involving technology companies, is to be considered in identifying emerging technologies. This is significant. CFIUS—the jurisdiction of which was recently expanded by FIRRMA—is uniquely positioned to access confidential, sensitive information about proposed, consummated, withdrawn, and blocked transactions. This makes CFIUS privy not only to quantitative and qualitative data about transactions, but also—and perhaps more significant for the purpose of identifying emerging technologies essential to national security—the strategic, non-commercial or semicommercial objectives of foreign investors who seek to invest in or venture with U.S. businesses.
- It is likely that information brought to the interagency process through CFIUS will inform the early and ongoing interagency process, including whether and how some foreign parties are—in ways that are not transparent—linked to or are deemed to be acting on behalf of government or state-linked parties overseas. Given national security (and competition policy) concerns in the United States about foreign stateowned or linked companies, such information could be significant for export control decision-making purposes.

(6) The Problem of Legal, Policy, and Commercial Issue Mixing by Some Officials and Influencers

Particularly where China is concerned, there has been a tendency by some Administration officials, members of

Related MassPoint Publications

- <u>National Security-Based</u> <u>Restrictions on Foreign Access to</u> <u>U.S. Technology</u>, Oct. 2018.
- Legal and Reputation Risks in <u>Technology Supply Chains</u>, Aug. 2018.
- <u>Critical Minerals: Where National</u> <u>Security, Trade and Environmental</u> <u>Laws Will Meet</u>, Aug. 2018 (<u>tech</u> supply chains).
- <u>Canary in the Cobalt Mine:</u> <u>Glencore Corruption Probe May</u> <u>Not Be a One Off</u>, July 2018 (cobalt/tech supply chains).
- <u>ZTE: Was the Export Ban the Right</u> <u>Penalty</u>? May 2018.
- <u>U.S. Law as Trade War Weapon</u>, May <u>2018</u>.
- <u>U.S.-China Trade and Tech War on</u> <u>Three Fronts</u>, <u>May</u> 2018.
- <u>House Bill "Blocks Bailout" of ZTE</u> <u>After Export Ban</u>, May 2018.
- <u>Decoding Trump on Trade: Links</u> <u>Between Economic/Trade Issues</u> <u>and Military Security</u>, May 2018

Congress, and policy influencers to conflate legal, policy, and commercial issues identified by them as national security challenges. Such issue mixing has led and can again lead to actions and recommendations that are off the mark or have the potential to do more harm than good.

For example, in connection with the <u>export ban on ZTE</u> and its subsequent lifting, some prominent officials advocated for continuing to enforce the export ban to punish what they described as ZTE's "espionage" and malign cyber activities. But the ZTE case was, in essence, a sanctions enforcement case unrelated to "espionage" and cyber activities that trigger different laws, policies, and procedures. Such issue mixing, particularly if it carries over to efforts to regulate emerging technologies that are in development in the United States and abroad (including, notably, in China), can cause confusion, delay, and result in misplaced policy recommendations (although the interagency nature of the process will presumably provide helpful checks). Commentators should be mindful of the ways in which some prominent voices and decision makers have discussed and approached important legal and regulatory issues.

<u>Hdeel Abdelhady</u> is MassPoint's Founder and Principal and also teaches a law school course on the regulation of foreign access to U.S. technology. She can be reached at habdelhady@masspointpllc.com.

NOTES

¹ § 1751(3), Export Controls Act of 2018, Part 1 of the Export Control Reform Act of 2018 (ECRA) passed as part of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Aug. 13, 2018) (NDAA). The Export Controls Act of 2018 will be referred to as ECRA.

² The Foreign Investment Risk Review and Modernization Act of 2018 (**FIRRMA**), which was enacted with ECRA as Title 17 of the NDAA, "Review of Foreign Investment and Export Controls," updates and expands the jurisdiction of the Committee on Foreign Investment in the United States to review, on national security grounds, certain foreign investment. Like ECRA, FIRRMA requires that assessments of foreign investment take into account their potential to diminish the United States' technological edge.

³ § 1753, ECRA.

⁴ Id. at § 1758(a).

⁵ Id. at § 1758(b).

⁶ FIRRMA's definition of "critical technologies" includes "emerging and foundation technologies controlled pursuant to section 1758" of ECRA.

⁷ Defense Production Act of 1950, 50 U.S.C. § 4552 (as amended by FIRRMA).

⁸ Id.

⁹ Scope of the Export Administration Regulations, 15 C.F.R. § 734.8

¹⁰ NSDD 189 defines fundamental research as "basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons." NSDD 189 provides, as a matter of policy, that the appropriate mechanism for national security-based control of fundamental research is classification and, accordingly, prohibits the placing of restrictions "upon the conduct or reporting of federally-funded fundamental research that has not received national security classification, except as provided in applicable U.S. Statutes."

¹¹ See, e.g., Hdeel Abdelhady, <u>Trade Wars: Restricting Foreign Access To US Technology</u>, Law360, October 19, 2018 (subscription req'd); also available <u>here</u>, via <u>MassPoint PLLC</u> (discussing five categories of measures adopted or under consideration to restrict foreign access to U.S. technology: "(1) foreign investment, (2) supply chain exclusions, (3) limits on participation in academic and other research, (4) legal or political curbs on U.S. technology access or transfers through third countries, and (5) countermeasures against foreign control of raw materials essential to technological manufacturing and innovation.").

¹² Department of Justice, Attorney General Jeff Sessions's China Initiative Fact Sheet, Nov. 1, 2018. Mr. Sessions announced the initiative and the "fact sheet" bears his name, but the China Initiative is led by the Assistant Attorney General for the National Security Division at the DOJ and staffed with other DOJ personnel. Thus, Mr. Sessions' departure presumably will have little to no impact on the China Initiative, which advances Trump Administration policy.

¹³ For example, as <u>discussed here</u>, the National Security Strategy identifies, among other technologies, "autonomous technologies, gene editing, new materials, nanotechnology, [and] advanced computing technologies.

¹⁴ National Research Council and National Academy of Engineering, *Emerging and Readily Available Technologies and National Security: A Framework for Addressing Ethical, Legal, and Societal Issues*, The National Academies Press (2014), 45, available at https://doi.org/10.17226/18512.

¹⁵ Id.

¹⁶ *Id.* at § 1753(c).

¹⁷ ECRA

¹⁸ *Id.* at § 1756(d)(1).

¹⁹ Id. at § 1756(d)(3).

20 § 1758(a)(1), ECRA.

²¹ Consideration of these sources is required by ECRA at § 1758(a)(2).