Chapter 14: Technology Protection

Blueprint for Action

This Blueprint for Action provides detail for how the United States must craft technology protection policies to ensure it retains existing advantages in technology areas with national security applicability but avoids stifling innovation. U.S. research, entrepreneurship, and talent development remain the key ingredients of success. However, as dual-use technologies become more important to U.S. national security, the margin of U.S. technological advantage narrows, and foreign efforts to acquire American know-how and technology increase, the United States must also reexamine how it can protect its commercial and academic ecosystem from foreign exploitation. The United States faces substantial challenges in adapting its technology protection regime to address threats related to emerging, dual-use technologies such as artificial intelligence (AI) without hindering the free flow of commerce or its open research environment, both of which are systemic U.S. strengths. This Blueprint for Action proposes reforms for (1) modernizing export controls and investment screening and (2) protecting the U.S. research environment in ways which are consistent with U.S. national security, commercial interests, and values.

Modernizing Export Controls and Investment Screening

How the U.S. Government regulates competitors' access to sophisticated U.S. technologies with national security applications will be one of the principal challenges of current and future geoeconomic competition. The United States must modernize its export control and investment screening regimes to better address the challenges posed by dual-use emerging technologies, to include AI. These reforms are necessary to allow the government to implement technology protection policies in ways which maximize their impact on the military capabilities of U.S. strategic competitors and minimize any resulting harms to U.S. industry.

Recommendation

Recommendation: Clearly State the Overarching Principles to Guide Future U.S. Dual-Use Technology Protection Policies

The U.S. Government must clearly state the principles that will guide future U.S. decisions regarding policies to protect critical technologies. This will enable more consistent and cohesive technology protection policies and provide clarity to industry regarding how the government intends to utilize these regulatory tools in the current competitive environment, thereby reducing uncertainty for U.S. businesses. No such framework currently exists.

Action for the President:

- **Issue an Executive Order outlining the principles which will guide U.S. policies for protecting dual-use technologies.[1]**
    - The President should issue an Executive Order to clarify guiding principles which will guide U.S. policies to protect critical dual-use technologies, including AI. The Executive Order should include the following guiding principles:
        - U.S. technology controls will not supplant investment and innovation.
        - U.S. strategies to promote and protect U.S. technology leadership will be integrated and mutually reinforcing.
        - The United States will be judicious in applying export controls to AI-related technologies, targeting discrete chokepoints and coordinating policies with allies.
        - The United States will broaden investment screening to protect AI-related technologies.

Recommendation

Recommendation: Enhance U.S. Capacity to Carry Out Effective Technology Protection Policies

Departments and agencies responsible for protecting U.S. technologies lack the organizational and technical capacity to design and implement effective policies to prevent the transfer of the national security–sensitive components of emerging technologies such as AI. They suffer from a dearth of technical talent needed to identify effective new policies and lack the analytical capacity to enforce their policies efficiently, especially on dual-use goods. Filling these gaps in key elements of the Executive Branch––particularly in the Departments of Commerce, the Treasury, and State––will enhance the government's ability to craft targeted export controls that have the greatest strategic impact and pose the least harm to U.S. competitiveness.

Actions for the Department of Commerce:

- **Designate a network of FFRDCs and UARCs to serve as a shared technical resource on export controls.[2]**
    - To deepen its internal technical expertise, the Department of Commerce should establish a network within existing federally funded research and development centers (FFRDCs) and university-affiliated research centers (UARCs) to provide technical expertise to all departments and agencies for issues relating to export controls on emerging technologies. This network should be coordinated by the Department of Commerce and encompass a regional distribution of FFRDCs and UARCs that are either located in U.S. technology hubs or have significant expertise in emerging technologies.
    - As an initial step, the Department of Commerce should identify the FFRDCs and UARCs with existing expertise in emerging technologies under consideration for export controls. This should be followed by a request for funding in the Fiscal Year (FY) 2022 President's Budget to support and expand work of FFRDCs and UARCs focusing on export controls.

- **Require all new technology protection rules on emerging technologies to be coordinated with existing technical advisory groups that include outside experts.[3]**
    - The Secretary of Commerce should require that the Bureau of Industry and Security (BIS) solicit and receive feedback on any proposed controls on emerging or foundational technologies, to include proposed rules and regulations, from the Emerging Technology Technical Advisory Committee (ETTAC) and any other relevant technical advisory groups.[4] More frequent and effective use of such existing advisory committees would provide flexible technical expertise to key departments, help prevent publishing counterproductive controls, and ensure that policymakers hear the perspective of industry and academia before controls go into effect.

Actions for the Departments of Commerce, the Treasury, and State:

- **Expedite and automate export licensing and CFIUS filing processes.[5]**
    - The Departments of Commerce and the Treasury should partner with FFRDCs, UARCs, and other contracted entities to build an integrated, smart system for analyzing export license applications and filings with the Committee on Foreign Investment in the United States (CFIUS). This system should utilize AI to conduct a preliminary analysis of filings and attempt to score levels of risk before human review. In the near term, this would help identify which transactions are very low risk and which are very high risk to aid subsequent human review. In the longer term, it could prove more accurate than human review and make decisions without human involvement, allowing for precise, rapid, and less labor-intensive reviews.
- **Encourage allies to implement legal reforms authorizing them to implement unilateral export controls and enhance investment screening procedures.**
    - The Departments of State and Commerce must urge all allies which have not already done so to pass domestic legislation to overhaul their export control regimes, increasing their bureaucratic capacity and providing them the authorities to implement unilateral export controls. Currently, many allies lack such domestic legal authorities and instead defer all decisions about regulations to multilateral organizations such as the Wassenaar Arrangement and the European Union.[6] These reforms are needed to allow allies to implement targeted, rapid, and effective export controls on emerging dual-use technologies, which are evolving quickly. Technology protection regimes on globally available products are only as strong as their weakest link, necessitating U.S. cooperation with allies and strong allied regulatory capacity. This builds on existing work, which has been productive and should continue with an immediate focus on countries that have a strong domestic emerging technology base and weak regulatory regimes.[7]
    - The Departments of State and the Treasury should expedite efforts to enhance the investment screening capabilities of close allies and partners. Existing efforts have shown some success but now require increased urgency, given the threats allies face from adversarial capital and the U.S. desire to exempt some firms in allied nations from certain CFIUS requirements.[8] State and the Treasury should also regularly share data about patterns in investment flows in the United States and allied countries to assist allied efforts to block predatory investments and illustrate the nature of the threat.
- **Ensure that the offices responsible for export controls and investment screening policies have sufficient resources and technical capacity.**

- The Departments of Commerce, the Treasury, and State must ensure that the offices responsible for designing and implementing export controls and investment screening provisions on emerging technologies are sufficiently resourced and have sufficient technical capacity. Agencies should rely on external sources such as FFRDCs, UARCs, and advisory boards for deep technical expertise on particular technologies. However, they also must ensure that the offices principally responsible for managing the policy processes regarding controls on these technologies have adequate staffing, resources, and baseline technical capacity to keep pace with the rapidly evolving security challenges associated with dual-use technologies.

Recommendation

Recommendation: Identify "Emerging" and "Foundational" Technologies Which Must Be Controlled, as Required by the Export Control Reform Act of 2018

The Export Control Reform Act of 2018 (ECRA) and the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) are intended to overhaul the U.S. export control and investment screening regimes to better accommodate emerging technologies. ECRA requires the Department of Commerce to develop a regular, formal interagency process to identify "emerging and foundational technologies that … are essential to the national security of the United States," and are not otherwise controlled.[9] Any such technologies identified by Commerce become subject to U.S. export controls, and any foreign investment in a U.S. company which "produces, designs, tests, manufactures, fabricates, or develops" one or more such technologies must be reviewed by CFIUS.[10] This list must be distinct from efforts within the Commission-proposed National Technology Strategy (NTS) to define emerging technologies key to U.S. national competitiveness and national security. The ECRA list must be more narrowly defined and focused only on specific technologies for which export controls are necessary, whereas the TCC and NTS' focus should be on identifying broader technologies and particular platforms in which continued U.S. leadership is essential.

However, as of March 2021, the Department of Commerce has yet to identify a single emerging or foundational technology as mandated by ECRA. While there is reason to be judicious in developing this list, given its implications on U.S. industry, and Commerce faces legitimate capacity and resourcing limitations, the magnitude of the delay is unacceptable. The delay has garnered bipartisan criticism, created uncertainty for firms working in fields that could be labeled as emerging or foundational technologies, and delayed the government's ability to either control the export of, or more importantly gain insight into transactions involving, critical technologies that are not otherwise controlled.[11]

Identifying this list of technologies is critical to enabling the United States to fully implement both ECRA and FIRRMA. As ECRA and FIRRMA are structured, until the Department of Commerce defines a technology which is not otherwise controlled as "emerging and foundational" as part of this review process, with rare exceptions CFIUS cannot require foreign companies to disclose non-controlling investments in U.S. technology

firms. Although the Commission also recommends breaking CFIUS' reliance on this ECRA list for mandatory disclosures (see recommendations on reforming CFIUS for emerging technology competition, below), currently Commerce's delay in identifying such technologies is hindering the full implementation of both ECRA and FIRRMA.

Action for the Department of Commerce:

- **Direct the Bureau of Industry and Security to develop proposed rules containing initial lists of both "emerging" and "foundational" technologies by December 31, 2021.**[12]
    - The Secretary of Commerce should direct the BIS to work with the U.S. interagency to develop initial versions of the lists of "emerging" and "foundational" technologies by December 31, 2021. Beyond 2021, these lists should be regularly revised in an iterative manner to meet ECRA's mandate to Commerce to continually refine the lists. As part of this iterative review process, Commerce must also regularly engage with industry as technologies develop and mature. Finalizing initial versions of these lists, if properly scoped and defined, would control critical technologies, clarify to industry how Commerce intends to implement ECRA, and ensure that such technologies are included within CFIUS.

Recommendation

Recommendation: Reform CFIUS for Emerging Technology Competition

CFIUS is not currently postured to address the range of threats that the United States faces from adversarial capital from strategic competitors such as China and Russia. The Department of the Treasury has little insight into Russian and Chinese investments in U.S. emerging technology firms, as CFIUS filings are still largely voluntary for non-controlling investments in industries such as AI, semiconductors, quantum computing, and telecommunications equipment. While FIRRMA took positive steps in broadening CFIUS' authorities, it also left critical gaps in the investment screening regime. Additional steps are necessary to enable CFIUS to protect sensitive U.S. industries from adversarial capital, while ensuring the continued free flow of capital from trusted investors from allied nations.

Action for Congress:

- **Amend CFIUS' authorizing legislation to require competitors to disclose investments in "sensitive technologies" to CFIUS.**
    - Congress should amend CFIUS' authorizing legislation to mandate CFIUS filings for all non-controlling investments from "countries of special concern" in "sensitive technologies." The Commission recommends that the legislation:
        - Define "countries of special concern" as states subject to export restrictions pursuant to section 744.21 of title 15 within the Code of Federal Regulations (China, Russia, and Venezuela) or any state that the Secretary of State designates as a state sponsor of terrorism (Iran, North Korea, and Syria).[13]
        - Require the Treasury Department to define a separate list of "sensitive technologies" for the purposes of CFIUS. Only investors from "countries of

special concern" would be required to submit CFIUS filings for investments in "sensitive technologies." Treasury currently lacks authorities to broaden CFIUS' mandatory filing requirements, which are linked to lists of technologies that are export controlled.[14]

- Mandating CFIUS filings from select competitors in a broader set of sensitive industries—such as national security—relevant applications of AI, semiconductors, quantum computing, and advanced telecommunications equipment—will provide the Treasury with better visibility into Russian and Chinese investments in U.S. firms in key sectors. This allows CFIUS to operate with more precision and insight and focus attention on the riskiest investments.
- Additionally, de-linking CFIUS disclosure requirements from export controls recognizes that there are instances in which it may be appropriate to screen investments prior to enacting export controls.[15] Without this change, the only way to increase such disclosure requirements would be to place export controls on entire industries, which would significantly hamper commerce.

Action for the Department of the Treasury:

- **Expedite CFIUS exemption standards for allies and partners and create fast tracks for exempting trusted investors.**
  - The Department of the Treasury should issue clear guidance regarding what investment screening policies allied nations must implement to achieve CFIUS-exempted status.[16] Clearly defining the standards for investment screening mechanisms in foreign nations necessary for investors to be exempted from CFIUS will create a powerful incentive for allied nations to adopt stronger screening mechanisms against adversarial capital. The sooner the Treasury takes this action, the more impact it will have on allied regulations. The Treasury should prioritize engagement with Five Eyes intelligence-sharing partners, Japan, South Korea, India, Israel, Singapore, Taiwan, and the European Union to enable investment from allied nations in U.S. high-tech firms.
  - Treasury should also issue new regulations creating a waiver for "trusted investors" from foreign countries that have a strong track record of CFIUS approval to exempt them from or lessen their CFIUS requirements. Currently there is no certification for investors with a trusted track record, and CFIUS treats foreign investors that are submitting for the first time the same as ones which have already submitted and been approved 100 times. Creating such a waiver would allow CFIUS to fast-track investments from low-risk, trusted investors with a strong history of CFIUS approval, facilitating legitimate foreign investment and focusing CFIUS' resources on higher-risk investments.

Recommendation

Recommendation: Utilize Targeted Export Controls on Key Semiconductor Manufacturing Equipment

Although the Commission believes that export controls on AI algorithms would likely be ineffective given their widespread availability and commercial use, export controls on specific hardware components are capable of constraining competitors' AI capabilities with national security applications and slowing their advancement. Policymakers must

be judicious in their application of such controls, as sweeping controls on general-use semiconductors are likely to cause substantial damage to the U.S. semiconductor industry and could have a net negative effect on overall U.S. competitiveness in microelectronics. However, targeted controls on key components that only the United States—or the United States and a small group of close allies—produce which are essential for cutting-edge defense applications could have a significant strategic impact at a relatively minimal cost.

The primary target for such controls should be select, high-end semiconductor manufacturing equipment (SME) needed to produce high-end chipsets, particularly photolithography equipment.[17] China is the world's largest importer of SME, accounting for 29% of global imports from 2014 to.2018, and none of the largest or most sophisticated SME manufacturing firms are located in China.[18] Simultaneous to implementing such controls, as discussed in Chapter 13 of this report, the United States should also fund efforts to prioritize the domestic development and manufacturing of SME tools and components needed to produce chips at scale at the 3nm node and beyond.[19]

Action for the Departments of Commerce and State:

- **Align the export control policies of the United States, the Netherlands, and Japan to restrict the export of high-end SME to China, including EUV and ArF immersion lithography equipment.[20]**
    - The Departments of State and Commerce should work to align the export control policies of the United States, the Netherlands, and Japan regarding high-end SME, particularly extreme ultraviolet lithography (EUV) equipment and argon fluoride (ArF) immersion lithography equipment, which is capable of producing chips at the 16nm node and below.[21] All three states should establish a policy of presumptive denial of export licenses for exports of such equipment to China.[22] This should include EUV scanner tools as well as specialized components for those tools, such as resist processing tools and EUV light sources, mirrors, and laser amplifiers. If such controls are effective, it will be difficult for China's government to cultivate indigenous, cutting-edge semiconductor fabrication capabilities and will degrade its advanced trailing-edge fabrication capabilities by complicating equipment repairs. Coupled with the refundable investment tax credit to promote U.S. semiconductor leadership recommended in Chapter 13 of this report, this will further the Commission's proposed U.S. policy goal of remaining two generations ahead of China in cutting-edge microelectronics design and fabrication.[23]
- **Assess the effectiveness of existing U.S. export controls on SME on China's semiconductor industry and assess whether targeted controls on additional equipment are viable and necessary.**
    - The Departments of Commerce and State should assess the effectiveness of existing U.S. export controls on SME on China's indigenous advanced semiconductor industry. Pending the results of that review and whether the Netherlands and Japan agree to align controls related to EUV and ArF immersion equipment, the United States could subsequently consider controls on additional SME chokepoints. If existing controls have failed to slow China's development of advanced fabrication capabilities, the United States could consider implementing controls on other targeted equipment chokepoints controlled by firms in allied

countries, such as atomic layer etching tools in conjunction with Japan and the United Kingdom.[24]

Recommendation: Utilize End-Use Export Controls to Prevent Malicious Use of AI

Recommendation

Export controls that restrict transfer of dual-use items for specific end uses will not be effective at preventing technology transfer to determined adversaries, but they can still play a role in preventing the involvement of U.S. firms and technology in human rights abuses. For specific, high-end, dual-use equipment prone to facilitating uses of AI which enable human rights abuses, such as mass surveillance, U.S. firms should be required to certify that the equipment will not be used for specific nefarious ends and keep logs of their transactions. End-use controls and reporting requirements would not substantially delay sales and present a lower barrier to commerce compared to list-based controls. Requiring companies to self-certify and self-report could deter U.S. firms from knowingly enabling bad behavior abroad.

Action for the Department of Commerce:

- **Implement end-use controls and reporting requirements to prevent the use of high-end U.S. AI chips in human rights violations.**
    - The Department of Commerce should implement end-use controls on high-end U.S.-designed or -manufactured AI chips for use in mass surveillance applications and institute reporting requirements on sales of such chips to China. The controls should be targeted only at very high-end or specialized chips, such as specific high-performing GPUs, ASICs, or FPGAs that exceed a certain high-performance threshold.[25] Commerce would, by necessity, update this threshold as chips continue to improve.
    - Any firm that sells such chips to China should have to certify that the chips will not be used for any designated human rights abuses. Firms that sell such chips should also be required to provide quarterly reports to BIS listing all chip sales, in what quantity, and to which company. This will facilitate U.S. government tracking of chips that are most likely to facilitate abusive uses of AI and deter companies from selling chips to businesses that they know are engaging in such behavior.[26]

Protecting the U.S. Research Environment

The United States needs comprehensive and resourced interagency measures to counter adversarial threats to its research environment, especially from China. Efforts must be supported by technically versed intelligence collection, analysis, and dissemination on threats in the Science & Technology (S&T) space. Promising steps have been initiated through the National Counterintelligence Task Force and the Office of Science and Technology Policy.[27] However, it is imperative to holistically improve the way the government postures itself and equips the research community—in academia and the private sector—to counter threats and uphold the integrity of open research.

Recommendation

Recommendation: Build Capacity to Protect the Integrity of the U.S. Research Environment

Actions for Congress:

- **Pass a modified version of the Academic Research Protection Act.[28]**
    - Congress should pass the Academic Research Protection Act (ARPA) with a modification that would mandate and execute standardization of grant processes across federal research-funding agencies.[29]
        - The ARPA would establish a National Commission on Research Protection; establish an open-source intelligence clearinghouse relating to foreign threats to academia overseen by the Director of National Intelligence; improve guidance from the Departments of State and Commerce on export control responsibilities; and develop a Federal Bureau of Investigation (FBI) outreach strategy to promote information sharing on threats to the academic community.
        - The proposed modification would mandate development and implementation of a uniform application process and database across all Executive agencies that award R&D grants. This would enable effective oversight by grant-awarding agencies, allow for automated auditing, and support investigative efforts by federal law enforcement.
- **Establish a government-sponsored independent entity focused on research integrity.**
    - Congress should authorize the sponsorship of a university-affiliated research center (UARC) to act as a center of excellence on research integrity and provide information and advice on research security.
    - The entity should bridge the gap between the government and academic and private-sector research institutions and lower the barriers for research organizations to independently conduct compliance and informed risk assessments.
    - The UARC mandate should be to:
        - Maintain open-source materials to serve university vetting of international engagement and risk management, including databases and risk-assessment tools;
        - Provide tailored guidance to research organizations for decision support;
        - Conduct comprehensive studies and regular reports on the state of foreign influence on U.S. research;
        - Undertake independent investigations on research integrity;
        - Develop education materials and tools for U.S. research institutions to build annual training and compliance initiatives; and
        - Manage dialogue with stakeholder communities and provide a venue for information sharing.

Action for the Director of National Intelligence:

- **Strengthen channels for information sharing with the research community.**
    - In concert with the open-source intelligence clearinghouse relating to foreign threats to academia directed by the ARPA legislation, the Director of National Intelligence should support increased information and intelligence sharing with designated personnel at research organizations to share actionable information on specific threats. This would provide organizations the ability to swiftly take steps to mitigate risks.

Recommendation

Recommendation: Coordinate Research Protection Efforts Internationally with Allies and Partners

The United States should build a coalition of like-minded nations committed to the principle of open fundamental research and the associated values of research integrity—sidelining nations and organizations that do not abide by the values that provide the foundation for international innovation and science cooperation.[30]

Action for the Office of Science and Technology Policy:

- **Foster international dialogue around research protection and integrity.**
    - The Office of Science and Technology Policy, through the National Science and Technology Council, should work in coordination with Department of State's Office of Science and Technology Cooperation and Office of the Science and Technology Adviser to foster discussions with like-minded allies and partners focused on mitigating detrimental academic collaboration with China's People's Liberation Army (PLA)-affiliated and other high-risk entities. This should involve the establishment of an annual meeting of relevant education, science, and industry ministers to deepen research collaboration and coordinate on issues related to intellectual property and research security.

Action for the Department of Justice:

- **Strengthen information-sharing venues.**
    - The Department of Justice (DOJ) and FBI, in coordination with Intelligence Community partners, should strengthen channels for information sharing on threats and best practices on research protection and coordinate multilateral responses to enforce research security.

Action for the Department of State:

- **Reinforce global norms around a commitment to open fundamental research.**
    - Through international dialogues on research security and associated diplomacy, the Department of State should reinforce global norms around commitment to open

fundamental research,[31] as described in the United States in the National Security Decision Directive (NSDD)-189, the *National Policy on the Transfer of Scientific, Technical and Engineering Information*.[32]

Recommendation

Recommendation: Bolster Cybersecurity Support to Research Institutions

Protection of research data and intellectual property from cyber-enabled theft is perhaps the most important and actionable layer of security for the U.S. R&D environment. This is particularly true for AI, when theft of training data or trained models essentially provides malicious actors access to a final product. Federal investments in priority emerging technology research areas such as AI should be accompanied by a requirement and support for institutions—whether academic or private sector—to implement cybersecurity measures that adequately guard research data from cyber-enabled theft.

Actions for U.S. grant-making agencies:

- **Incentivize cybersecurity standards and best practices for grant-receiving research institutions.**
    - U.S. grant-making agencies should provide incentives to research institutions to ensure that necessary practices, based on the existing NIST cybersecurity framework,[33] as well as governance processes are in place to protect sensitive research data.
        - Reporting structures and information flows of research institutions should be structured to raise cybersecurity as a critical issue for senior management and facilitate internal checks and audits. This includes senior leadership awareness of cyber threats, risk assessments, and active preventive measures.
        - U.S. grant-making agencies should make available incentives for research institutions that demonstrate adherence to cybersecurity standards and best practices.
        - Universities, research institutions, and other recipients of federal research funding should be required to periodically demonstrate that they are adhering to cybersecurity best practices. For government-owned and -sponsored laboratories, adherence to best practices, such as requiring critical data to be encrypted at rest and in transit, should be mandated and audited on a routine basis.
- **Support increased information sharing.**
    - Research institutions receiving federal research dollars that do not already participate should be encouraged to join the Research and Education Networks Information and Sharing Analysis Center (REN-ISAC)[34] or an alternate ISAC, through which they can share information on threats and mitigation, benefit from automated threat-sharing tools, and have access to peer-assessment services to strengthen security postures.
    - Similarly, research institutions should be made aware and encouraged to take advantage of the cybersecurity services offered by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), to include automated indicator sharing[35] and enhanced cybersecurity services.[36]

Action for the Federal Bureau of Investigation:

- **Share real-time, actionable threat information with research institutions.**
    - The FBI Cybersecurity Division should work closely with and share timely, anonymized threat information with REN-ISAC and research institutions to help them take active measures to counter cyber attacks and mitigate vulnerabilities.

Action for the Department of Homeland Security:

- **Support research cybersecurity information sharing similar to that of critical infrastructure.**
    - The Department of Homeland Security, CISA, and National Cybersecurity and Communications Integration Center[37] should support the level of information sharing with research institutions as they do with critical infrastructure and the Financial Services ISAC.[38]

Action for the Office of Science and Technology Policy:

- **Support secure data storage.**
    - OSTP should broker commercial cloud credits[39] for universities to establish an ability to support secure data storage for research groups and laboratories conducting work known to be of high interest to foreign adversaries. This would provide an ability for universities to protect their sensitive research in a manner that does not require a significant capital investment.

Recommendation: Counter Foreign Talent-Recruitment Programs

Recommendation

China uses foreign talent-recruitment programs to achieve a "high ground" of AI experts.[40] Rather than pursue legitimate competition for scientific talent through attractive job offers, China's talent-recruitment plans are designed in a manner that contradicts U.S. norms of research integrity, violates rules around disclosure, and creates vectors for technology transfer.[41] The FBI and Intelligence Community assess that "participants are often incentivized to transfer to China the research they conduct in the United States, as well as other proprietary information to which they can gain access."[42] There is an urgent need to reinforce standards around disclosure of conflicts of interest and commitment and to create mechanisms that enable a heightened level of transparency and accountability.[43] This applies to researchers' individual transparency and institutional accountability, as well as to the government in identifying problematic affiliations and enforcing standards. Currently, U.S. grant-making agencies lack common processes, coordination, and compliance mechanisms to enable this level of transparency and effective oversight.[44]

Action for the Office of Science and Technology Policy:

- **Standardize grant application and recording processes.**
    - The Office of Science and Technology Policy (OSTP), in coordination with the Office of Management and Budget, should provide advice and coordination to the Executive Branch to make uniform the grant application and recording processes across Federal agencies that fund external research.
    - OSTP should advise and coordinate with agencies to ensure agencies embrace a government-wide standard for grant proposal documentation, requiring machine-readable formats that facilitate automation to identify fraud.[45] This would enable effective oversight by grant-awarding agencies, allow for automated auditing, and support investigative efforts by federal law enforcement.

Actions for Congress:

- **Mandate and resource compliance operations.**
    - Congress should require and resource U.S. grant-making agencies to maintain compliance operations that can enforce standardized disclosure and accountability measures. Through periodic vetting and monitoring, grant-making agencies can provide a layer of accountability to enforce disclosure and protection policies.[46]
- **Amend the Foreign Agent Registration Act.**
    - Congress should amend the Foreign Agent Registration Act (FARA)[47] to require any individual or entity involved in the recruitment of U.S. nationals for a foreign talent program[48] to register as a foreign agent. This requires Congress to add a new category of activity to the legislation.

Actions for Department of Justice:

- **Update filing regulations to support an amended FARA.**
    - Should Congress amend FARA legislation as proposed above, DOJ, in its implementing regulations, should identify specific information required from individuals involved in recruitment for foreign talent programs to ensure that the U.S. government has adequate visibility into foreign countries' talent recruitment activities in the United States.
    - DOJ regulations should include methods for individuals and organizations to appeal a determination that they are subject to registration under this FARA expansion.
- **Publicly identify U.S.-based entities and foreign government proxies that serve as recruitment networks, platforms, or brokers.**
    - To help raise awareness among researchers and research institutions, and reinforce transparency, Federal law enforcement and other relevant agencies should identify entities involved in recruitment activities for foreign talent programs and require their registration through the FARA (if amended).
    - This effort must be accompanied by an associated appeal process for organizations to contest the need to register from identification.

Recommendation: Limit Collaboration with PLA-Affiliated Persons and Entities

Recommendation

PLA-affiliated universities and research labs send personnel abroad, with the overarching aim to obtain knowledge that can directly feed defense research and development priorities. Visiting scholars or students from PLA institutions often downplay their ties to the military or deliberately obscure affiliation by using alternate, external names for their home institutions that do not mention military or defense mandates.[49]

The government should take actions through designation of institutions of concern and heightened visa vetting to assist universities in making risk assessments around research collaborations—becoming an effective partner in protecting research integrity.

Action for the Director of National Intelligence:

- **Create an open-source database of organizations that have a history of improper technology transfer, intellectual property theft, or cyber espionage.[50]**
    - The Director of National Intelligence, in coordination with law enforcement partners, should create a queryable database of academic institutions and other organizations that have a history of improper technology transfer, intellectual property theft, or cyber espionage. This resource should serve the research community and inform risk assessments of research organizations when entering collaborative arrangements. It would represent an expansive, open-source view of research institutions of concern, countering efforts to obscure military affiliations through adoption of innocuous institutional aliases.
    - This must be accompanied by an associated appeal process for organizations to contest their inclusion in the database.

Action for the President:

- **Limit entrance of researchers with military and intelligence affiliations from countries of concern.**
    - The President should issue an order to the Secretary of State and Secretary of Homeland Security to implement a requirement for special review of visas for advanced-degree students and researchers with ties to research institutions affiliated with foreign military and intelligence organizations of designated countries of concern.[51]
        - This should be paired with penalties that ban entry to any visa applicants found to have intentionally obscured institutional affiliations.

Action for the Department of State:

- **Resource special review measures.**
    - Consular officers should be provided with adequate training, reference resources, analytical support, and time to conduct the special review.

Blueprint for Action: Chapter 14 - Endnotes

[1] A draft text of such an Executive Order is included in an Annex to this Blueprint for Action. This Executive Order also includes directives pertaining to most other export control–related recommendations in this Blueprint for Action.

[2] Additional details for this recommendation are also contained within the draft Executive Order included as an Annex to this Blueprint for Action.

[3] Additional details for this recommendation are also contained within the draft Executive Order included as an Annex to this Blueprint for Action.

[4] The ETTAC contains roughly 20 leading technical experts from prominent U.S. technology and defense firms, universities, and think tanks. However, it has been underutilized by Commerce; ETTAC did not hold a single meeting between June 2018 and May 2020. *Emerging Technology Advisory Committee*, Bureau of Industry and Security (last accessed Jan. 2, 2021), https://tac.bis.doc.gov/index.php/ettac-home.

[5] Additional details for this recommendation are also contained within the draft Executive Order included as an Annex to this Blueprint for Action.

[6] The Wassenaar Arrangement, a multilateral body with 42 participating states, is the primary international forum responsible for aligning policies on dual-use export controls. However, because it operates by consensus and includes Russia, is slow to react to new technologies and developments, and is non-binding, the Wassenaar Agreement must not be the exclusive forum in which the United States and allies negotiate export control provisions on dual-use technologies. *About Us*, The Wassenaar Arrangement (last accessed Jan. 2, 2021), https://www.wassenaar.org/about-us/; *Second Quarter Recommendations*, NSCAI at 68-69 (2020), https://www.nscai.gov/previous-reports/.

[7] The Chapter 15 Blueprint for Action and associated Annex reinforce this recommendation and illustrate how these efforts should fit into a broader technology diplomacy strategy.

[8] See Chris Darby, et al., *Mitigating Economic Impacts of the COVID-19 Pandemic and Preserving U.S. Strategic Competitiveness in Artificial Intelligence*, NSCAI at 14-15 (May 19, 2020), https://www.nscai.gov/white-papers/covid-19-white-papers/; *Second Quarter Recommendations*, NSCAI at 69, 75-77 (July 2020), https://www.nscai.gov/previous-reports/.

[9] 50 U.S.C. § 4817(a)(1)(A).

[10] 50 U.S.C. § 4565(a)(4)(B)(iii)(II); 85 Fed. Reg. 3112, *Provisions Pertaining to Certain Investments in the United States by Foreign Persons*, U.S. Department of Treasury: Office of Investment Security (Jan. 17, 2020) https://www.federalregister.gov/documents/2020/01/17/2020-00188/provisions-pertaining-to-certain-investments-in-the-united-states-by-foreign-persons.

[11] *New Controls on Emerging Technologies Released, While U.S. Commerce Department Comes Under Fire for Delay*, Gibson Dunn (Oct. 27, 2020), https://www.gibsondunn.com/new-controls-on-emerging-technologies-released-while-us-commerce-department-comes-under-fire-for-delay/; Letter from U.S. Senators Tom Cotton and Charles E. Schumer to Secretary Wilbur Ross, Department of Commerce (Nov. 18, 2019), https://www.cotton.senate.gov/imo/media/doc/191118_Cotton_Schumer_ECRA%20Letter%20to%20Sec.%20Ross%20copy.pdf.

[12] Additional implementation details for this recommendation are also contained within the draft Executive Order included as an Annex to this chapter.

[13] *State Sponsors of Terrorism*, U.S. Department of State (last accessed Jan. 2, 2021), https://www.state.gov/state-sponsors-of-terrorism/.

[14] As discussed in the following recommendation, due to the Department of Commerce's delay in identifying export controls on "emerging and foundational technologies," as required under the Export Control Reform Act of 2018 (ECRA), CFIUS' mandatory filing requirements have largely not expanded to emerging technology industries.

[15] For instance, for early-stage technology venture investments, particularly those that do not yet produce specific products, export controls have historically been ineffective, but investment screening would still have value. See Michael Brown & Pavneet Singh, *China's Technology Transfer Strategy*, Defense Innovation Unit Experimental at 24 (Jan. 2018), https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf.

[16] CFIUS regulations released in January 2020 created an exception for non-controlling technology, infrastructure, and data (TID) investments for investors tied to "excepted foreign states," with Australia, Canada, and the United Kingdom forming the initial list. The regulations require that excepted foreign states implement their own process to analyze foreign investments for national security risks and to facilitate coordination with the United States on investment screening by February 2022. However, Treasury has yet to publish the criteria CFIUS will use when determining whether additional countries can qualify as "excepted foreign states" in the future. See 31 C.F.R. 800.218 (2020), https://home.treasury.gov/system/files/206/Part-800-Final-Rule-Jan-17-2020.pdf.

[17] The detailed reasons why high-end SME and photolithography equipment in particular represents the best target for such controls are described in Chapter 14 of this report.

[18] John Verwey, *The Health and Competitiveness of the U.S. Semiconductor Manufacturing Equipment Industry*, SSRN at 5, 8 (July 1, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3413951.

[19] See Chapter 13 of this report and its associated Blueprint for Action for additional details on recommendations to support the U.S. microelectronics industry, to include U.S. development of SME.

[20] Additional details for this recommendation are also contained within the draft Executive Order included as an Appendix to this chapter.

[21] EUV lithography equipment is the only type of lithography equipment capable of mass manufacturing chips at the 5nm node or potentially below. ArF immersion lithography equipment is the only other type of tool capable of mass producing chips at the 28nm node or below, with more sophisticated ArF immersion equipment capable of nodes under 16nm. See Saif Khan, *Securing Semiconductor Supply Chains*, Georgetown Center for Security and Emerging Technologies at 20 (Jan. 2021), https://cset.georgetown.edu/research/securing-semiconductor-supply-chains/.

[22] In 2019, the United States put significant pressure on the Netherlands to block a sale of EUV lithography equipment from Dutch firm ASML to Chinese firm SMIC. The contract expired before the equipment was delivered, although the Netherlands has not stated whether or not it will approve future sales. See Alexandra Alper, et al., *Trump Administration Pressed Dutch Hard to Cancel China Chip-Equipment Sale: Sources*, Reuters (Jan. 6, 2020), https://www.reuters.com/article/us-asml-holding-usa-china-insight/trump-administration-pressed-dutch-hard-to-cancel-china-chip-equipment-sale-sources-idUSKBN1Z50HN.

[23] Increasing the competitiveness of the cutting-edge U.S. microelectronics fabrication industry would create new market opportunities for SME firms, which could offset any potential losses resulting from decreased access to the Chinese market due to export controls. This is particularly important for allied governments that may be hesitant to impose export controls on equipment which will hurt key domestic companies without simultaneously providing them access to new markets or growing existing markets.

[24] Saif Khan, *Securing Semiconductor Supply Chains*, Georgetown Center for Security and Emerging Technologies at 20 (Jan. 2021), https://cset.georgetown.edu/research/securing-semiconductor-supply-chains/.

[25] GPUs are graphics processing units, ASICs are application-specific integrated circuits, and FPGAs are field-programmable gate arrays.

[26] The Chapter 15 Blueprint for Action reinforces this recommendation and illustrates how these efforts should fit into a broader technology diplomacy strategy.

[27] Specifically, the Joint Committee on Research Environments within the National Science and Technology Council. See *NSTC*, The White House (last accessed Jan. 1, 2021), https://www.whitehouse.gov/ostp/nstc/.

[28] H.R. 8346, Academic Research Protection Act, 116th Cong. (2020), https://www.congress.gov/bill/116th-congress/house-bill/8346.

Blueprint for Action: Chapter 14 - Endnotes

[29] This could mirror a provision for development of a uniform grant application process across research-funding agencies proposed in S. 3997, Safeguarding American Innovation Act, 116th Cong. (2020), https://www.congress.gov/bill/116th-congress/senate-bill/3997/text.

[30] Notably, two-thirds of overseas professional associations that transfer technology to China are located outside the United States. See Ryan Fedasiuk & Emily Weinstein, *Overseas Professionals and Technology Transfer to China*, Center for Security and Emerging Technology at 2 (July 21, 2020), https://cset.georgetown.edu/research/overseas-professionals-and-technology-transfer-to-china/. One-third of Thousand Talents awardees are located outside the United States, mainly in the U.K., Germany, and Singapore. See Ryan Fedasiuk & Jacob Feldgoise, *The Youth Thousand Talents Plan and China's Military*, Center for Security and Emerging Technology at 4 (Aug. 2020), https://cset.georgetown.edu/research/the-youth-thousand-talents-plan-and-chinas-military/. Two-thirds of awardees for some of China's largest scholarship programs are outside the United States. See Andrew Imbrie & Ryan Fedasiuk, *Untangling the Web: Why the US Needs Allies to Defend Against Chinese Technology Transfer*, Brookings Institution at 3 (April 2020), https://www.brookings.edu/research/untangling-the-web-why-the-us-needs-allies-to-defend-against-chinese-technology-transfer/. Leaders in Canada, the Netherlands, U.K., Japan, and India have in recent years publicly raised concerns around security risks related to research collaborations with China. Remco Zwetsloot, *China's Approach to Tech Talent Competition: Policies, Results, and the Developing Global Response*, Center for Security and Emerging Technology at 8 (April 2020), https://cset.georgetown.edu/research/chinas-approach-to-tech-talent-competition-policies-results-and-the-developing-global-response/.

[31] This could build on a concept currently under consideration by the National Science Foundation to establish and formalize an international code of conduct around shared principles in research integrity and then fund collaborative research in accordance with said principles.

[32] The directive defines fundamental research as: "'Fundamental research' means 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." The key provision of NSDD-189 remains today: "It is the policy of this Administration that, to the maximum extent possible, the products of fundamental research remain unrestricted. It is also the policy of this Administration that, where the national security requires control, the mechanism for control of information generated during federally funded fundamental research in science, technology and engineering at colleges, universities and laboratories is classification." *National Policy on the Transfer of Scientific, Technical and Engineering Information*, NSDD-189 (Sept. 21, 1985), https://fas.org/irp/offdocs/nsdd/nsdd-189.htm.

[33] *Cybersecurity Framework*, NIST (last accessed Feb. 1, 2021), https://www.nist.gov/cyberframework.

[34] REN-ISAC (last accessed Jan. 2, 2021), https://www.ren-isac.net/.

[35] *Automated Indicator Sharing*, Cybersecurity and Infrastructure Security Agency (CISA) (last accessed Feb. 10, 2021), https://www.cisa.gov/automated-indicator-sharing-ais.

[36] *Enhanced Cybersecurity Services (ECS)*, Cybersecurity and Infrastructure Security Agency (last accessed Feb. 10, 2021), https://www.cisa.gov/enhanced-cybersecurity-services-ecs.

[37] *Cyber Incident Response*, CISA (Oct. 27, 2020), https://www.cisa.gov/cyber-incident-response.

[38] *Information Sharing and Awareness*, CISA (Dec. 8, 2020), https://www.cisa.gov/information-sharing-and-awareness.

[39] The National Science Foundation's CloudBank program could be leveraged as a model. See CloudBank, https://www.cloudbank.org/.

[40] William C. Hannes & Huey-meei Chang, *China's Access to Foreign AI Technology*, Center for Security and Emerging Technology (CSET) at 9-10 (Sept. 2019), https://cset.georgetown.edu/wp-content/uploads/CSET_China_Access_To_Foreign_AI_Technology.pdf.

[41] The Office of Science and Technology Policy defines foreign government talent-recruitment programs as "an effort directly or indirectly organized, managed, or funded by a foreign government to recruit science and technology professionals or students (regardless of citizenship or national origin)." *Enhancing the Security and Integrity of America's Research Enterprise*, Office of Science and Technology Policy at 18 (June 2020), https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/07/Enhancing-the-Security-and-Integrity-of-Americas-Research-Enterprise.pdf.

[42] Testimony of John Brown, Assistant Director, Counterintelligence Division, Federal Bureau of Investigation, delivered before the U.S Senate Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations, *Hearing on Securing the U.S. Research Enterprise from China's Talent Recruitment Plans* at 2 (Nov. 19, 2019), https://www.hsgac.senate.gov/imo/media/doc/Brown%20Testimony.pdf. In some cases, the Chinese government appears to have rewarded scientists caught stealing technology through talent-recruitment programs, Alex Joske, *Hunting the Phoenix*, Australian Strategic Policy Institute at 8 (2020), https://www.jstor.org/stable/resrep26119.1.

[43] A National Science Foundation-commissioned JASON study on fundamental research security found that "disclosure of activities presents our main defense against foreign influence, especially that involving rewards, deception, and coercion." *Fundamental Research Security*, JASON at 31 (Dec. 6, 2019), https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf.

[44] *Threats to the U.S. Research Enterprise: China's Talent Recruitment Plan*, U.S. Senate Permanent Subcommittee on Investigations (Nov. 2019), https://www.hsgac.senate.gov/imo/media/doc/2019-11-18%20PSI%20Staff%20Report%20-%20China's%20Talent%20Recruitment%20Plans.pdf.

[45] This mirrors a recommendation from the U.S. Senate Permanent Subcommittee on Investigations. See *Threats to the U.S. Research Enterprise: China's Talent Recruitment Plan*, U.S. Senate Permanent Subcommittee on Investigations at 11 (Nov. 2019), https://www.hsgac.senate.gov/imo/media/doc/2019-11-18%20PSI%20Staff%20Report%20-%20China's%20Talent%20Recruitment%20Plans.pdf.

[46] The National Institutes of Health's recent investments in this capability could serve as a model for others, scaled in terms of an agency's level of funding.

[47] 22 U.S.C. § 611 et seq.

[48] This will require a clear definition of a foreign talent program, distinct from standard internationally funded research opportunities. The Office of Science and Technology Policy defines foreign government talent recruitment programs as "an effort directly or indirectly organized, managed, or funded by a foreign government to recruit science and technology professionals or students (regardless of citizenship or national origin)." *Enhancing the Security and Integrity of America's Research Enterprise*, Office of Science and Technology Policy at 18 (June 2020), https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/07/Enhancing-the-Security-and-Integrity-of-Americas-Research-Enterprise.pdf.

[49] Glenn Tiffert, *Global Engagement: Rethinking Risk in the Research Enterprise*, The Hoover Institution at 12 (2020), https://www.hoover.org/sites/default/files/research/docs/tiffert_globalengagement_full_0818.pdf.

[50] If Congress passes the Academic Research Protection Act, this initiative could be a component of the open-source intelligence clearinghouse on threats to academia created through the legislation.

[51] This is recommended as an update to Presidential Proclamation 10043 that automatically suspends F or J visas to study or conduct research for Chinese nationals affiliated with the Chinese government military-civil fusion strategy. See Donald J. Trump, *Proclamation on the Suspension of Entry as Nonimmigrants of Certain Students and Researchers from the People's Republic of China*, The White House (May 29, 2020), https://trumpwhitehouse.archives.gov/presidential-actions/proclamation-suspension-entry-nonimmigrants-certain-students-researchers-peoples-republic-china/. This order would provide for a case-by-case, risk-based review of potentially concerning applications from a broader group of designated countries.

Chapter 14 Annex: Technology Protection

Draft Executive Order on Export Control on Principles Guiding U.S. Policies for Protecting Dual-Use Technologies

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to promote U.S. innovation and leadership in emerging and foundational technologies while protecting U.S. national security, it is hereby ordered as follows:

Section 1. Policy. It is the policy of the United States that export controls and investment screening mechanisms must be used in targeted, clearly defined, and strategic ways to protect U.S. national security, in pursuit of the broader policy of promoting U.S. innovation and leadership in emerging and foundational technologies, to include dual-use technologies such as artificial intelligence (AI).

The United States must be tailored and discrete in implementing export controls on dual-use emerging technologies such as AI. To ensure maximum effectiveness and minimize the adverse impact on U.S. industry, the U.S. Government should be guided by the following principles:

(1) **Principle One: Export Controls Cannot Supplant Investment and Innovation.** Technology protection policies are intended to slow U.S. competitors' pursuit and development of key strategic technologies for national security purposes, not stop them in their tracks. The United States must cultivate investment in these technologies through direct federal funding or changes to the regulatory environment in order to preserve existing U.S. advantages.

(2) **Principle Two: U.S. Strategies to Promote and Protect U.S. Technology Leadership Must Be Integrated.** The U.S. strategy to protect emerging technologies, including but not limited to AI, must be integrated with targeted efforts to promote U.S. leadership in such technologies. When choosing to implement controls, the United States should simultaneously consider policies to spur domestic research and development (R&D) in key industries to partially offset the resulting costs to U.S. firms, create alternative global markets, or encourage new investment to strengthen the U.S. industrial position.

(3) **Principle Three: Export Controls Must Be Targeted, Strategic, and Coordinated with Allies.** In devising new export controls on widespread and dual-use technologies such as AI, the United States must be careful and selective in the implementation of export controls. To ensure maximum effectiveness and minimize the adverse impact on U.S. industry, the U.S. Government should be guided by the following three-part test:

a. Export controls must be targeted, clearly defined, and focused on choke points where they will have a strategic impact on the national security capabilities of competitors but smaller repercussions on U.S. industry.

b. Export controls must have a clear strategic objective, seeking to deter competitors from pursuing paths that endanger U.S. national security interests, and account for the projected cost and timeframe for competitors to create a domestic alternative.

c. Export controls must be coordinated with key U.S. allies which are also capable of producing the given technology, in order to effectively restrict the supply to adversaries and also prevent circumstances in which unilateral controls cut off U.S. market access but competitors are able to purchase the same technology from other countries.

(4) **Principle Four: The United States will be judicious in its use of export controls but broaden investment screening on critical and emerging technologies.** While broad and sweeping export controls on AI and other dual-use emerging technologies could result in significant blowback on U.S. industry, which would harm overall U.S. strategic competitiveness, investment screening presents opportunities to take a more proactive regulatory approach while minimizing risk to U.S. industry. Provided the United States can continue approving benign transactions expeditiously, enhancing investment screening presents significant potential to blunt concerning transfers of technology.

Section 2. Objective. In 2018, the Congress enacted the Export Control Reform Act of 2018 (ECRA) and the Foreign Investment Risk Reduction Modernization Act of 2018 (FIRRMA) to provide the U.S. Government with additional mechanisms to control exports and screen investments. The U.S. Government must take steps to provide the private sector and foreign governments with clarity about the application of these laws to emerging and foundational technologies and enhance U.S. national security in the process.

Section 3. Establishment of Interagency Task Force on Emerging and Foundational Technologies. (a) Pursuant to Section 1758 of ECRA, there is hereby established an Interagency Task Force on Emerging and Foundational Technologies (Task Force) to identify emerging and foundational technologies that are essential to the national security of the United States and are not critical technologies described in clauses (i) through (v) of 50 U.S.C. 4565(a)(6)(A).

(b) The Task Force shall be chaired by the Secretary of Commerce (Chair) and consist of senior-level officials from the following Executive departments and agencies (agencies) designated by the heads of those agencies:

(i) Department of State;

(ii) Department of the Treasury;

(iii) Department of Defense;

(iv) Department of Energy; and

(vi) such other agencies as the President, or the Chair, may designate.

(c) The Chair shall designate a senior-level official of the Department of Commerce as the Executive Director of the Task Force, who shall be responsible for regularly convening and presiding over the meetings of the Task Force, determining its agenda, and guiding its work in fulfilling its functions under this Order, in coordination with the BIS at the Department of Commerce.

Section 4. Functions of the Task Force.

(a) The Task Force shall meet regularly to identify emerging and foundational technologies that are essential to the national security of the United States for purposes of establishing export controls and investment screening mechanisms, as appropriate, related to those technologies.

(b) Within 120 days, the Task Force shall finalize lists of emerging and foundational technologies pursuant to section 1758 of ECRA. The Secretary of Commerce shall thereafter issue proposed rules on emerging and foundational technologies and proceed expeditiously to issue final rules at the conclusion of the notice and comment period.

(c) The Task Force shall review the lists of emerging and foundational technologies and issue amendments as needed on no less than an annual basis.

Section 5. Process for Identifying Emerging and Foundational Technologies. (a) In identifying emerging and foundational technologies pursuant to this Order, the Task Force shall consider information from multiple sources, including:

(i) publicly available information;

(ii) classified information, including relevant information provided by the Director of National Intelligence;

(iii) information relating to reviews and investigations of transactions by the Committee on Foreign Investment in the United States under 50 U.S.C. 4565; and

(iv) information provided by the advisory committees established by the Secretary to advise the Under Secretary of Commerce for Industry and Security on controls under the Export Administration Regulations, including the Emerging Technology Technical Advisory Committee (ETTAC).

(b) In identifying emerging and foundational technologies pursuant to this Order,

the Task Force shall take into account:

(i) the development of emerging and foundational technologies in foreign countries;

(ii) the effect that export controls imposed pursuant to this section may have on the development of such technologies in the United States;

(iii) the effectiveness of export controls imposed pursuant to this section on limiting the proliferation of emerging and foundational technologies to foreign countries; and

(iv) the policy and principles reflected in section 1 of this Order.

Section 6. Improving Coordination with Expert Advisory Groups. (a) The Secretary of Commerce shall review existing technical advisory committees (TACs) at the Department of Commerce, including the ETTAC, to ensure that each TAC is composed of members from industry and academia with deep subject-matter expertise to assess the need for export controls for emerging and foundational technologies.

(b) The Secretary of Commerce, as Chair of the Task Force, shall ensure that the Task Force has solicited and received feedback from the ETTAC and other relevant TACs at the Department of Commerce on the text of any proposed or final rule on emerging or foundational technologies, prior to issuance of such rule.

(c) The Secretary of Commerce shall ensure that senior officials at the Departments of State and the Treasury are granted non-voting observer access at all ETTAC meetings.

Section 7. Improving International Coordination on Export Controls on Semiconductor Manufacturing Equipment. Within 180 days, the Secretary of State, in consultation with the Secretary of Commerce and the Secretary of Defense, shall host a multilateral engagement with senior-level representatives of Japan, the Netherlands, and, if deemed appropriate, other U.S. allies and partners that produce semiconductor manufacturing equipment (SME), including EUV lithography equipment and ArF immersion lithography equipment, listed by the Wassenaar Arrangement or identified by the Task Force. The purpose of this meeting will be to align export licensing policies toward a presumptive denial of export licenses for exports of semiconductor manufacturing equipment to China. The Secretary of State shall provide a report to the President within 60 days of the meeting assessing:

(i) whether U.S. allies and partners are currently exporting such equipment to China;

(ii) what steps each country that manufactures such equipment must take to ensure its regulatory regime is aligned with that of the United States, and its willingness to take those steps; and

(iii) whether additional opportunities exist to strengthen international cooperation on export controls on SME which are consistent with the policy and principles reflected in Section 1 of this Order.

Section 8. Engaging Technical Experts for Export Control Review. (a) The Secretary of Commerce, in consultation with the Secretaries of the Treasury and Defense, shall establish a network within existing Federally Funded Research and Development Centers (FFRDCs) and University Affiliated Research Centers (UARCs) to provide technical expertise to all departments and agencies for issues relating to export controls and investment screening related to emerging and foundational technologies. The network shall encompass a regional distribution of FFRDCs and UARCs located in areas of the United States with a concentration of technology expertise in emerging and foundational technologies.

(b) Individuals selected to participate in the network shall provide real-time technical input to all policy discussions on export controls and review of export control license applications, including those of the Task Force, those conducted pursuant to EO 12981 or a successor order, and any other interagency policy discussions pertaining to export controls, as well as the investment screening processes of the Committee on Foreign Investment in the United States (CFIUS).

Section 9. Automating Export Control and Investment Screening Reviews. The Secretaries of Commerce and the Treasury shall task the aforementioned network with exploring using AI-based systems to assist in the evaluation of applications for export control licenses and CFIUS filings and shall provide a report to the President on the use of AI-based systems for such purposes within 180 days. This report shall include an evaluation of:

(i) how AI-based systems could assist existing review processes;

(ii) whether incorporating such systems could enhance the accuracy and speed of the review processes;

(iii) whether relevant Departments and Agencies have sufficient quantity and quality of data to train AI-based review systems, and how existing data can be improved;

(iv) what information technology infrastructure inside relevant Departments and Agencies needs to be improved to fully utilize such systems; and

(iv) an approximate timeline and cost for deploying a system or systems, and the projected savings per year in labor-hours once deployed.

Section 10. General Provisions. (a) Nothing in this Order shall be construed to impair or otherwise affect:

(i) the authority granted by law, regulation, Executive Order, or Presidential Directive to an executive department, agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.