Questions for the Record

The Biden Administration's PRC Strategy

July 20, 2023

Representative Mike Gallagher – District WI-8

Witness – Thea Kendler

1. How many waivers and to which companies have been granted from the October 7, 2022 rule on semiconductors?

The Bureau of Industry and Security's (BIS) rule, which was announced on October 7, 2022, and published as an interim final rule (87 Fed. Reg. 62186 (Oct. 13, 2022)) in the Federal Register on October 13, 2022, is part of our ongoing efforts to protect U.S. national security and foreign policy interests. This rule imposed restrictive new export controls on certain advanced computing integrated circuits, transactions related to supercomputer end uses, and transactions involving certain entities on the Entity List. In addition, the rule imposed new controls related to the production of advanced semiconductors in the People's Republic of China (PRC or China). Specifically, the rule imposed new PRC-wide restrictions on exports of (i) certain tools essential to produce advanced chips, (ii) any U.S. tools, components, or other items to a PRC semiconductor fabrication facility that produces advanced logic or memory chips, and (iii) any item for the development or production of PRC indigenous semiconductor tools. The rule also imposed a license requirement on U.S. persons providing support related to items not subject to BIS jurisdiction that will be used to develop or produce chips at a facility that fabricates advanced chips.

Generally, license applications related to these controls are reviewed with a presumption of denial. However, the October 7, 2022, rule made clear that this presumption of denial does not apply to exports of semiconductor manufacturing items destined to end users in China that are headquartered in the United States or in certain allied countries (Country Groups A:5 or A:6). License applications involving such end users are considered on a case-by-case basis, taking into account factors including technology level, customers, and compliance plans. Consequently, if authorized, certain

multinational companies operating in the PRC may continue certain activities on a case-by-case basis. Providing authorizations under the specified criteria furthers the national security and foreign policy objectives of the October 7 rule by addressing the likely harm of supply chain disruptions to the United States and our allies if manufacturing ceases at certain facilities in the near term. Additionally, these authorizations also deter companies in allied countries from seeking to exclude U.S. commodities and technologies subject to our jurisdiction in their manufacturing, which would only harm long-term U.S. technology leadership, which itself is part of our national security interests.

Since the rule's announcement on October 7, 2022, BIS has taken a number of steps to ensure its effectiveness. This includes initiating a public comment period, issuing related FAQs, and engaging closely with international partners in coordinating approaches to export controls of these and other items to the PRC. In the intervening months key international supplier governments have independently and publicly released information related to new restrictions they intend to put in place through their domestic legal systems to restrict the export of advanced semiconductor manufacturing equipment. The United States will continue to monitor these developments and will continue to engage with these and other international partners.

As numerous open-source analyses make clear, the PRC's ability to access items and obtain support for the production of the most advanced semiconductors has been impacted. The Department understands that export controls must stay ahead of an evolving threat environment, which is why we are constantly and relentlessly vigilant, in coordination with our interagency partners, in reviewing available classified and open-source information, to enforce and appropriately update our export controls to address the threats posed by the PRC. While the Department recognizes the need to act quickly, which it did by issuing an interim final rule last year, it must also act deliberately. The Department will make additional adjustments, as appropriate, to our controls in response to public comments and in consultation with our interagency partners.

BIS has acted to further update the October 2022 rule by issuing additional updates on October 17, 2023. Additional information regarding the October 2023 updates and how they build on the October 2022 rule are available on BIS's website at:

https://www.bis.doc.gov/index.php/policy-guidance/advanced-computing-and-semiconductor-manufacturing-items-controls-to-prc.

This request for information pertaining to specific authorizations or applicants is restricted from release pursuant to Section 1761(h) of the Export Control Reform Act of 2018 (ECRA). BIS will respond to a separate formal request made by the Chairman or Ranking Member on their official Committee letterhead to furnish certain restricted information to the Committee. Information released to the Committee pursuant to Section 1761(h) is subject to further restrictions on disclosure outlined in the law.

2. Do any of Huawei's operations in the United States pose an unacceptable risk to the national security of the United States or the security and safety of United States persons?

For answers to 2-13 please see response to 14.

3. Do any of ZTE's operations in the United States pose an unacceptable risk to the national security of the United States or the security and safety of United States persons?

4. Do any of DJI's operations in the United States pose an unacceptable risk to the national security of the United States or the security and safety of United States persons?

5. Do any of WeChat's operations in the United States pose an unacceptable risk to the national security of the United States or the security and safety of United States persons?

6. Do any of BGI's operations in the United States pose an unacceptable risk to the national security of the United States or the security and safety of United States persons?

7. Do any of Quectel's operations in the United States pose an unacceptable risk to the national security of the United States or the security and safety of United States persons?

8. Do any of Fibocom's operations in the United States pose an unacceptable risk to the national security of the United States or the security and safety of United States persons?

9. Do any of Dahua's operations in the United States pose an unacceptable risk to the national security of the United States or the security and safety of United States persons?

10. Do any of CRCC's operations in the United States pose an unacceptable risk to the national security of the United States or the security and safety of United States persons?

11. Do any of LOGINK's operations in the United States pose an unacceptable risk to the national security of the United States or the security and safety of United States persons?

12. Do any of ZPMC's operations in the United States pose an unacceptable risk to the national security of the United States or the security and safety of United States persons?

13. Do any of Hikvision's operations in the United States pose an unacceptable risk to the national security of the United States or the security and safety of United States persons?

14. Do any of Inspur's operations in the United States pose an unacceptable risk to the national security of the United States or the security and safety of United States persons?

Response to questions 2-14:

Many of the entities identified in your questions are either presently on the Entity List maintained by BIS, which identifies foreign parties that have been, are, or may become involved in activities contrary to U.S. national security and foreign policy interests, or, in the case of ZTE, remain subject to the terms and conditions of the 2018 Superseding Settlement Agreement. The Entity List provides citations to the Federal Register notice that describes the activities that led to that entity's listing, as well as the items subject to license requirements and license review policy applicable to that entity.

As a general matter, the Entity List is a notification to exporters that there has been a determination, based on specific, articulable evidence, that these entities have, are, or pose a risk of becoming engaged in activities that are contrary to U.S. national security or foreign policy interests and that export transactions with those entities are subject to additional scrutiny. A firm's presence on the Entity List or other restrictions imposed on such firms should at a minimum be a red flag for U.S. companies and individuals when it comes to engaging in transactions with those firms.

Your questions also use the "undue or unacceptable risk" language from Executive Order (EO) 13873. The EO authorizes the Department to review and, as necessary, prohibit or approve, subject to mitigation measures, transactions that involve Information and Communications Technology and Services (ICTS) that is "designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary" and that poses undue or unacceptable risks to U.S. national security. This authority, delegated by the Department to BIS, includes the ability to review ICTS transactions involving connected software applications. To date the majority of these reviews have resulted from referrals from other Executive Branch agencies, but the authorities allow the Department to undertake reviews on its own initiative. BIS has not publicly announced any final determinations related to ICTS transactions that may or may not be under review at this time, nor can it confirm or deny any potential ongoing investigations. Nonetheless, BIS

would be happy to provide information and briefings on any final determinations as appropriate in the future.

The Department of Commerce and our interagency partners remain vigilant with respect to any entity based in the PRC that has been, is currently, or is at high risk of becoming involved in activities contrary to U.S. national security and foreign policy interests.

15. Does the Department of Commerce believe PRC investments in open-source software like RISC-V represents a threat to the United States?

As you know, RISC-V International is a non-profit organization that has been working to develop open-source semiconductor technology standards that are open to a variety of stakeholders globally. The Department is aware of concerns related to the potential for exploitation by foreign adversaries of open-source software, which is generally not subject to export controls, and other platforms. The Department is working to assess potential risks as well as to develop and consider whether there are appropriate actions under Commerce authorities for addressing any potential concerns.

From a national security perspective, the development of electronic design software and/or of a chip architecture is only one component of the semiconductor production supply chain—adversaries also need to be able to produce the chips that are designed. The Department has acted strategically to restrict the PRC's ability to obtain the items and technologies necessary to manufacture advanced semiconductors that present national security concerns. On October 7, 2022, the BIS issued a rule imposing PRC-wide restrictions on semiconductor manufacturing equipment (SME), advanced semiconductors, as well as related items and supercomputing entities based in the PRC. This rule focused on impairing the PRC's ability to produce and/or obtain the advanced computational capacity supported by advanced semiconductors that can enable the development of artificial intelligence (AI) for military and other purposes that present national security concerns. On October 17, 2023, BIS issued three additional rules imposing restrictions on additional SME, advanced semiconductors, as well as adding several PRC-based entities with military ties engaged in the advanced semiconductor design and manufacturing sector to the Entity List. These actions further refine the controls issued in 2022 and expand restrictions on the PRC's ability to obtain items

necessary to produce advanced chips. Additional information on these rules is available on BIS's website at: https://www.bis.doc.gov/index.php/policy-guidance/advanced-computing-and-semiconductor-manufacturing-items-controls-to-prc.

In addition, over the past year certain like-minded international partner governments have independently acted to place similar restrictions on the PRC's ability to obtain items for the production of advanced semiconductors, further strengthening the actions taken by the Department.

While there are valid concerns that certain technologies could be transferred to the PRC, U.S. export controls on advanced semiconductors, semiconductor manufacturing tools, and other items particular to the PRC are making it difficult for firms in the PRC to actually produce advanced semiconductors at scale.

At the same time that the Department is acting strategically to protect U.S. national security interests, it must also consider how best to advance U.S. technological leadership. While RISC-V International differs from formal international standards setting bodies, the issues and concepts are similar. Ultimately U.S. national security and technological leadership are also advanced by robust U.S. industry and stakeholder participation in international standards setting bodies, which set the often invisible but critical standards that we rely on in our everyday lives. The United States should not cede international leadership, and U.S. persons should abide by all applicable export controls and related policies. The same holds true in the case of engagement with the development of RISC-V semiconductor technologies.

In fact, we have seen the impact of pulling back too quickly from such engagements. Failure to engage in such international collaborative activities risks ceding U.S. technological leadership. For example, in 2019, BIS added Huawei and a number of its non-U.S. affiliates to the Entity List. This addition, and subsequent actions to address Huawei's participation in international standards bodies, led to questions from U.S. industry, organizations, and other stakeholders about whether BIS licenses were required to release low-level technology for legitimate standards activities to parties on the Entity List. This uncertainty led U.S. companies to limit their participation in standards-related activities, including in areas critical to U.S. national security. In September of 2022, BIS issued an interim final rule (87 Fed. Reg. 55241 (September 09, 2022)) responding to these concerns that levels the playing field for U.S. companies to participate in all international standards setting organizations without

fear of legal penalties related to Entity List licensing requirements. Without such a standards-related authorization, U.S. companies would find themselves fighting uphill in the international technology marketplace—less able to engage in field-shaping discussions, less sure of the ways in which rules apply to vital standards activities, and less empowered to win market share for their innovations.

Ultimately, BIS and our interagency partners have experience working together with interagency partners, international governments, and industry, academia, and other stakeholders to carefully tailor export controls to promote U.S. technological leadership, and that experience can be applied similarly to the RISC-V context as well. BIS and our interagency partners will remain vigilant in evaluating the technological landscape for potential national security threats and will continue to act as appropriate to protect U.S. national security interests.

16. Should U.S. persons be allowed to conduct joint research with the PRC on RISC-V?

The United States should not cede international leadership, and U.S. persons should abide by all applicable export controls and related policies.

17. Do any of SMIC's operations in the United States pose an unacceptable risk to the national security of the United States or the security and safety of United States persons?

SMIC is on the Entity List maintained by BIS which identifies foreign parties that have been, are, or may become involved in activities contrary to U.S. national security and foreign policy interests.

While BIS's export control authorities generally do not extend to domestic economic activity, a firm's presence on the Entity List or otherwise subject to other restrictions should at a minimum be a red flag for U.S. companies and individuals when it comes to engaging in transactions with those firms.

The Department of Commerce and our interagency partners remain vigilant with respect to any entity based in the PRC that has been, is currently, or is at high risk of

becoming involved in activities contrary to U.S. national security and foreign policy interests.

18. Do any of YMTC's operations in the United States pose an unacceptable risk to the national security of the United States or the security and safety of United States persons?

By rule issued by BIS on December 16, 2022, YMTC is on the Entity List maintained by BIS which identifies foreign parties that have been, are, or may become involved in activities contrary to U.S. national security and foreign policy interests. BIS added YMTC on the basis of information indicating that the company presents a risk of diversion to parties on the Entity List.

While BIS's export control authorities generally do not extend to domestic economic activity, a firm's presence on the Entity List or otherwise subject to other restrictions should at a minimum be a red flag for U.S. companies and individuals when it comes to engaging in transactions with those firms.

The Department of Commerce and our interagency partners remain vigilant with respect to any entity based in the PRC that has been, is currently, or is at high risk of becoming involved in activities contrary to U.S. national security and foreign policy interests.

19. Do any of Shein's operations in the United States pose an unacceptable risk to the national security of the United States or the security and safety of United States persons?

The Department of Commerce and our interagency partners remain vigilant with respect to any foreign entity that has been, is currently, or may be at risk of becoming involved in activities contrary to U.S. national security and foreign policy interests. Under BIS's Information and Communications Technology and Services (ICTS) program in particular, additional controls, including mitigation measures or even prohibitions, can be placed on ICTS transactions, including those involving connected software applications, when the Department determines that such transactions pose

undue or unacceptable risks to national security or to the safety and security of U.S. persons.

20. Do any of Temu's operations in the United States pose an unacceptable risk to the national security of the United States or the security and safety of United States persons?

The Department of Commerce and our interagency partners remain vigilant with respect to any entity based in the PRC that has been, is currently, or may be at risk of becoming involved in activities contrary to U.S. national security and foreign policy interests. Under BIS's ICTS program in particular, BIS can seek to mitigate or, if necessary, prohibit ICTS transactions, including those involving connected software applications, where the ICTS is "designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction of a foreign adversary," and where the covered ICTS transaction poses undue or unacceptable risks" to U.S. national security or the safety and security of U.S. persons.

21. What is BIS's strategy for using ICTS authority?

The Department of Commerce, through BIS, is responsible for implementing the ICTS program. In particular, the ICTS program at BIS is charged with executing the policies and procedures outlined in EO 13873, "Securing the Information and Communications Technology and Services Supply Chain;" and EO 13984, "Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities." These EOs derive their authority from the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. § 1701, *et. seq*.

The program received its first substantial appropriations in December 2022 and has since worked to implement a robust hiring plan with a goal of increasing to 114 staff by the end of FY2024. As of March 2024, the program has hired 81 federal employees, and continues to bolster the program with contractors. In addition, 33 federal hiring actions are in progress.

The BIS ICTS program's mission, consistent with EO 13873, is to address undue or unacceptable national security risks posed by certain transactions involving ICTS that are "designed, developed, manufactured, or supplied by persons owned by,

controlled by, or subject to the jurisdiction or direction of, a foreign adversary." The regulations at 15 CFR Part 7, articulates the processes and procedures that the Secretary of Commerce uses to identify, assess, and address ICTS transactions and classes of ICTS transactions between U.S. persons and foreign persons that involve ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary.

The ICTS program is committed to leveraging these authorities to address undue or unacceptable risks to U.S. national security and to the safety and security of U.S. persons.

22. How many times has BIS reached a final determination for an ICTS Transaction? How many of these involved prohibiting a transaction? How many involved permitting a transaction pursuant to a mitigation agreement?

BIS has not publicly announced any final determinations related to ICTS transactions that may or may not be under review at this time, nor can it confirm or deny any potential ongoing investigations. BIS would be happy to provide information and briefings on any final determinations in the future, as appropriate.

23. Is BIS considering using ICTS authority for transactions involving TikTok? Is BIS considering using ICTS authority to permit any transactions involving TikTok, pursuant to mitigation?

The Administration takes seriously the national security risks related to certain technology products and services from China and other countries of concern. Information and Communications Technology and Services (ICTS) that are designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversary countries, including connected software applications, can threaten the national security, foreign policy, and economy of the United States. The Administration will strategically use its tools to address the national security risks presented by these threats – including the national security risks

associated with TikTok. The Department's ICTS program received its first substantial funding in December 2022. The program is ramping up hiring, to prevent undue or unacceptable risks to national security.

To put ICTS-related measures on the strongest possible footing, the Administration has consistently called for legislation that would codify in statute the ICTS authorities outlined in Executive Orders 13873 and 14034. Such legislation would strengthen and reinforce the federal government's ability to combat current and evolving threats, to safeguard the security and integrity of our ICTS supply chain, and to protect the American people and their data.

In that regard, the Department welcomes the opportunity to work with Congress on legislation that would address ICTS threats in a comprehensive way and protect our national security.

24. Why did BIS change the language in ICTS rules from "The extent to which identified risks have been or can be addressed by independently verifiable measures" to "The extent to which risks have been or can be mitigated using measures that can be verified by independent third parties"?

On June 16, 2023, the Department issued a final rule (88 FR 39353) implementing the provisions of Executive Order 14034, "Protecting Americans' Sensitive Data from Foreign Adversaries." This final rule responded to, and adopted changes based on, comments received in response to a Notice of Proposed Rulemaking (NPRM) issued on November 26, 2021 (86 FR 67379). The final rule amended the Securing the Information and Communications Technology Supply Chain regulations (15 CFR Part 7) to provide the additional criteria that the Secretary may consider when determining whether ICTS transactions involving connected software applications present undue or unacceptable risks (as those terms are defined in the regulations).

In the final rule, the Department revised the language to provide additional clarity in response to public comments received and to be more precise.

a. What sort of transactions have risks that could be mitigated using measures verified by independent third parties?

As a general matter, the ICTS program reviews, and can mitigate or even prohibit, ICTS transactions involving entities with an appropriate nexus to a foreign adversary and that may present risks such as:

> "sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States; . . . catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States; . . . or to the national security of the United States or the security and safety of United States persons."[1]

Depending on the facts of the transaction, it may be possible that the risks posed by a transaction could be mitigated using measures verified by independent third parties.

b. What are these risks?

See response to question 24a, above.

c. How does an entity qualify as an "independent third party"?

The ICTS program would need to assess the facts of a specific situation pursuant to the process outlined in the Securing the Information and Communications Technology and Services Supply Chain Regulations (15 CFR Part 7 to make such an assessment.

25. Are there any investments in the PRC or PRC companies by U.S. citizens or using U.S. dollars that pose an unacceptable

[1] EO 13873, Sec. 1(a)(ii).

risk to the national security of the United States or the safety and security of United States persons? If so, which ones specifically?

On August 9, 2023, President Biden issued Executive Order 14105, "Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern," which identifies semiconductors and microelectronics, quantum information technologies, and artificial intelligence sectors as important to U.S. national security and establishes a program for notification and, when appropriate, prohibition, on U.S. outbound investment into these sectors. Concurrently, the U.S. Department of the Treasury issued a notice of proposed rulemaking to solicit public comments on the program with the goal of implementing the Executive Order in the coming year.

26. Does CATL's licensing agreement with Ford pose an unacceptable risk to the national security of the United States or the safety and security of United States persons?

a. Are you concerned about CATL's licensing agreement for any other reason than national security? If so, what are those reasons?

The Department does not have any comment on this specific matter. However, any American company considering entering into a joint venture with a foreign party should carefully consider U.S. legal requirements, including export controls, prior to entering into any such agreement.

27. Are there any joint ventures between United States companies and PRC companies that pose an unacceptable risk to the national security of the United States or the security and safety of United States persons? Please list all that apply.

American companies seeking to enter into joint ventures with foreign partners should carefully consider U.S. legal requirements, including export controls, prior to entering into such agreements.

28. Are there any technology licensing agreements between United States companies and PRC companies that pose an unacceptable risk to the national security of the United States or the security and safety of United States persons? If so, which ones?

American companies seeking to enter into transactions with foreign partners should carefully consider U.S. legal requirements, including export controls, prior to entering into such agreements.

29. Does any aspect of UC Berkeley's research partnership with Tsinghua University or the Shenzhen Municipal Government pose an unacceptable risk to the national security of the United States or the security and safety of United States persons?

Our institutions of higher education are the crown jewel of our open society, and are also on the front lines of protecting our national security. BIS conducts outreach to universities to help educate them on the risks to national security of certain research collaborations, as well as the importance of complying with export controls and protecting American innovation.

BIS has generated numerous resources to assist compliance staff, researchers, and faculty in understanding the rules, their responsibilities, and to help them build effective compliance programs. For example, BIS's Export Enforcement has launched an Academic Outreach Initiative to provide selected research universities with dedicated liaisons and resources to ensure that they understand their compliance responsibilities. In addition, Export Administration's Office of Exporter Services also leads robust outreach efforts including seminars, webinars, and other outreaches to industry across

the country. We are committed to working with the academic community to protect U.S. national security while also protecting and advancing American innovation.

30. Do any research collaborations between the United States and PRC entities pose an unacceptable risk to the national security of the United States or the security and safety of United States persons? If so, which ones?

Research collaborations that are either ignorant of, or blatantly ignore, export controls present concerns for U.S. national security. Each research partnership in which a university or other entity participates should include a strong understanding of export controls and a robust compliance program.

The Bureau of Industry and Security has numerous resources available to industry and academic stakeholders to help them to build effective compliance programs. For example, BIS's Export Enforcement has launched an Academic Outreach Initiative to provide selected research universities with dedicated liaisons and resources to ensure that they understand their compliance responsibilities. In addition, Export Administration's Office of Exporter Services also leads robust outreach efforts including seminars, webinars, and other outreaches to industry across the country. BIS is committed to working with the academic and industry research community to protect U.S. national security while also protecting and advancing American innovation, and in cases where such rules and safeguards are either ignored or are inadequate and violations occur, BIS will not hesitate to use its enforcement authorities as appropriate.

31. Is it possible that a purchase or lease of land by a PRC company in close proximity to a facility openly owned or operated by the U.S. intelligence community could impair or damage the national security of the United States?

The Committee on Foreign Investment in the United States (CFIUS), which is chaired by the Treasury Department (Treasury), has authority to review certain real estate transactions, including those in close proximity to sensitive government facilities

or properties. While the Department is a member of CFIUS, this inquiry would be more appropriately directed to Treasury.

32. Is it possible that a purchase or lease of land by a PRC company in close proximity to a federally-funded research development center or a university-affiliated research center of the Department of Defense could impair the national security of the United States?

The Committee on Foreign Investment in the United States (CFIUS), which is chaired by the Treasury Department, has authority to review certain real estate transactions, including those in close proximity to sensitive government facilities or properties. While the Department is a member of CFIUS, this inquiry would be more appropriately directed to Treasury.

33. Is it possible that a purchase or lease of land by a PRC company in close proximity to a science and technology reinvention laboratories, as designated by the Secretary of Defense under 4121 of title 10, United States Code, could impair the national security of the United States?

As you may be aware, the Committee on Foreign Investment in the United States (CFIUS), which is chaired by the Treasury Department, has authority to review certain real estate transactions, including those in close proximity to sensitive government facilities or properties. While the Department is a member of CFIUS, this inquiry would be more appropriately directed to Treasury.

34. Is it possible that a purchase or lease of land by a PRC company in close proximity to critical infrastructure could impair the national security of the United States?

As you may be aware, the Committee on Foreign Investment in the United States (CFIUS), which is chaired by the Treasury Department, has authority to review certain

real estate transactions, including those in close proximity to sensitive government facilities or properties. While the Department is a member of CFIUS, this inquiry would be more appropriately directed to Treasury.

35. How is the Department of Commerce coordinating its efforts to deter the PRC from invading Taiwan with the Department of State and Department of Defense as well as any other relevant department? Please describe in as much detail as is possible in unclassified settings.

BIS continues to maintain comprehensive controls related to the PRC, including imposing a license requirement for all military and spacecraft items under our jurisdiction; all multilaterally-controlled dual-use items; a large number of dual-use items with extensive commercial applications if the item is intended, entirely or in part, for a military end use or military end user in the PRC; and all items under our jurisdiction, if the item is exported knowing it will be used in certain weapons of mass destruction (WMD) programs or if it is intended, entirely or in part, for military-intelligence end-uses or end-users in China. In addition, the Export Administration Regulations (EAR) prohibit certain U.S. person activities that would support WMD-related activities or military-intelligence end-uses or end-users in China absent authorization.

Thus, the EAR's licensing requirements for the PRC seek to prevent activities that threaten U.S. national security and foreign policy interests while allowing commercial activities that do not raise such issues. Export controls are an important tool in the U.S. government toolbox, but they are not the only tool. Any response to a kinetic action by the PRC against Taiwan would be a whole of government effort and BIS would take appropriate action, in coordination with the interagency and in consultation with allies and partners.

36. Can you provide specific examples of sensitive U.S. technologies that pose a national security threat and are

targeted by the Bureau of Industry and Security (BIS) to protect against PRC military modernization?

BIS maintains comprehensive controls related to the dual-use items with the most likely military utility to the PRC. They include imposing license requirements for all military and spacecraft items under our jurisdiction; all multilaterally-controlled dual-use items; a large number of dual-use items with extensive commercial applications if the item is intended, entirely or in part, for a military end use or military end user in the PRC; and all items under our jurisdiction if the item is exported knowing it will be used in certain WMD programs or if it is intended, entirely or in part, for military-intelligence end uses or end users in the PRC. In addition, BIS controls prohibit certain U.S. person activities that would support WMD-related activities or military-intelligence end uses or end users in the PRC absent authorization.

BIS controls are tailored to impose export license requirements based on the sensitivity of the item to be exported, the country of destination, the parties to the transaction, and the end use of the item. Some license requirements apply worldwide, including to our allies. Other license requirements apply more narrowly to a select group of countries, parties, or end uses.

All items subject to control for national security reasons require a license to the PRC and are scrutinized for the potential of diversion, particularly for items subject to Commerce's jurisdiction that have the greatest likely military utility. Effective October 29, 2020, BIS amended § 742.4(b)(7) of the EAR, which outlines changes to the licensing policy for items controlled for national security reasons when destined to the PRC.

The revised policy directs transactions to be assessed based on their potential for diversion to military end uses or end users and for the export, reexport, or transfer of items that would, "make a material contribution to the 'development,' 'production,' maintenance, repair, or operation of weapons systems, subsystems, and assemblies." See 85 Fed. Reg. 68448 (Oct. 29, 2020).

BIS develops and applies licensing policies that will apply to the export of items, destinations, parties, or end uses involved in the application. Approval of an export license application is a conclusion by BIS and its interagency partners that the

transaction is consistent with both the stated licensing policy and our national security and foreign policy objectives.

BIS will continue to evaluate the threat environment, technological advancements in a variety of industries and sectors, and other factors and will update controls as appropriate to protect U.S. national security and foreign policy interests, as evidenced by the controls announced on October 7, 2022, and related updates issued in October 2023, that seek to address concerns posed by the PRC's efforts to develop high performance computing capacity to train AI and related data and communications technologies that can be employed for military modernization and human rights abuses. Our restrictions related to advanced semiconductor manufacturing equipment, high performance chips and related items, and other measures outlined in those rules restrict the PRC's ability to obtain the tools and capabilities they desire for these activities and represent an expansion of our controls based on the present threat environment.

37. How does the BIS effectively control exports to advance U.S. strategic technology leadership and protect U.S. national security and foreign policy interests?

BIS advances U.S. national security and foreign policy interests by administering and enforcing an effective export control system. Essentially, our primary goal is to prevent malign actors from obtaining or diverting items, including sensitive technologies, for unauthorized purposes, to protect our national security, advance our foreign policy objectives, and maintain our leadership in science and technology, which itself is a national security imperative.

BIS develops and applies licensing policies that will apply to the export of items, destinations, parties, or end uses involved in the application. Approval of an export license application is a conclusion by BIS and its interagency partners that the transaction is consistent with both the stated licensing policy and our national security and foreign policy objectives.

BIS will continue to evaluate the threat environment, technological advancements in a variety of industries and sectors, and other factors and will update

controls as appropriate to protect U.S. national security and foreign policy interests, as evidenced by the controls announced on October 7, 2022, and related updates issued in October 2023, that seek to address concerns posed by the PRC's efforts to develop high performance computing capacity to train AI and related data and communications technologies that can be employed for military modernization and human rights abuses. Our restrictions related to advanced semiconductor manufacturing equipment, high performance chips and related items, and other measures outlined in those rules restrict the PRC's ability to obtain the tools and capabilities they desire for these activities and represent an expansion of our controls based on the present threat environment.

38. Could you elaborate on the process of reviewing license applications submitted by exporters and how the BIS collaborates with other agencies and partners to assess whether specific transactions align with or damage U.S. national security and foreign policy interests?

Decisions on export license applications submitted to the Department of Commerce undergo a rigorous interagency review that also includes the Departments of Defense, State, and Energy, in accordance with section 750.3 of the EAR and EO 12981, which outlines the export license application and review process. Within BIS, technical and policy experts review all elements of the application, including confirmation of the item classification, reliability of the parties to the transaction, and the licensing policy consistent with the EAR. In addition, applications are reviewed by our Office of Export Enforcement. BIS licensing process also includes a countersign feature to assure that no license can be validated without senior licensing officer review.

In Fiscal Year (FY) 2022, BIS processed more than 40,000 license applications. In the select instances where there is disagreement among the agencies on whether to approve the license, there is an established process for any agency to initiate further escalation from the working level to the Assistant Secretary level, and higher, for review. During FY 2022, approximately 1.1% of all applications submitted were appealed to the Assistant Secretary level. None were appealed to the Cabinet level or to the President, which would be the next steps in escalating a dispute. While the agencies

may have different perspectives on individual cases, we all bring helpful expertise to the process and can reach accommodation on almost all applications. And when we cannot, the interagency review and escalation process compels us to bring our best reasoning to the table to help shape U.S. export control policy.

39. What is the role of the intelligence community and law enforcement partners in the BIS' analysis of PRC efforts to obtain critical technology and advance its military capabilities?

BIS utilizes available open-source, proprietary, and classified information in coordination with the Intelligence Community as well as the U.S. and international law enforcement community. Where appropriate, we pursue criminal and civil penalties and use regulatory tools such as the Unverified List (UVL), which contains parties whose bona fides (i.e., legitimacy and reliability to engage in export transactions) BIS has been unable to verify and for whom no license exceptions may be used for exports, reexports, or transfers (in-country), or the Entity List to impose license requirements on parties of national security or foreign policy concern. BIS continually assesses PRC entities' compliance with our export controls and appropriate responses.

40. How does the BIS strategically use technology and entity-based controls to counter PRC Military-Civil Fusion Development Strategy and prevent the transfer of advanced commercial items that can be used in military applications?

The challenge posed by the PRC to U.S. national security and foreign policy interests is real, and BIS concurs with the 2024 Annual Threat Assessment by the Office of the Director of National Intelligence (ODNI), which asserts that "China seeks to become a world science and technology superpower and to use this technological superiority for economic, political, and military gains." In terms of export controls, Under Secretary Estevez's north star at BIS as it relates to the PRC is to ensure we are appropriately doing everything within BIS's power to prevent sensitive U.S. technologies from getting into the hands of the PRC's military, intelligence, security,

and services, or other parties that can divert or otherwise use U.S. sensitive technologies to undermine or erode U.S. technological leadership, enable human rights abuses, or engage in other activities that are contrary to our interests and values. Export controls are one of the many tools that the Biden Administration is using to coordinate and respond to the PRC's destabilizing activities. BIS is using controls to address the PRC's military-civil fusion strategy, which seeks to divert dual-use or commercial technologies to military uses. BIS is also using controls to confront the PRC's military modernization, WMD development, human rights abuses, and destabilization efforts in the Indo-Pacific. Addressing these concerns protects U.S. national security and advances our values and interests, as well as those of our allies and partners. This is a dynamic threat environment, and BIS is constantly evaluating existing authorities and thinking about how we can employ our tools to maximum effect.

As of December 9, 2023, nearly 800 entities in the PRC are listed on the Entity List, restricting their access to items subject to BIS's regulatory jurisdiction. Over 300 of these entities have been added during the Biden-Harris Administration. Furthermore, on October 7, 2022, Bureau of Industry and Security announced a rule (87 Fed. Reg. 62186) that imposed new controls on exports to the PRC) with respect to certain advanced computing chips, items for supercomputing applications, and items and support that could further the PRC's semiconductor production capabilities. BIS acted to further update the October 2022 rules by issuing additional updates on October 17, 2023. These rules address national security and foreign policy concerns related to China's military modernization, including its use of these technologies to enable the development of its weapons of mass destruction (WMD) programs, as well as its human rights abuses.

The most powerful computing capabilities—namely large-scale AI models and very powerful supercomputers, which are built on advanced semiconductors—present U.S. national security concerns because they allow the PLA to use AI to significantly improve the speed and accuracy of military decision making, planning, and logistics. They can also be used for cognitive electronic warfare, radar, signals intelligence, and jamming, and they can improve calculations in weapons design and testing, including for WMD. These capabilities can also create foreign policy concerns when they are used to support applications like facial or gait recognition surveillance systems for human

rights abuses. The PLA in particular has been open about how it views AI as critical to its military modernization efforts.

These are the national security and foreign policy considerations on which the advanced computing portion of the rule is based.

With respect to advanced computing, the October 7, 2022, rule made three changes. First, BIS implemented targeted restrictions on specific chips, and items containing such chips, that can be used in advanced computing and artificial intelligence applications. Through a new Foreign Direct Product (FDP) Rule, BIS also applied these controls to foreign-made chips and PRC chip designs meeting the relevant parameters. Second, BIS implemented controls for chips and other items that will be used in or for supercomputers in the PRC or supercomputers destined for the PRC. Through another new FDP Rule, this control also applies to certain foreign-made items when destined for PRC supercomputers, including foreign-made semiconductors. Third, BIS expanded the scope of controls for 28 PRC entities previously on the Entity List that are involved in supercomputer-related activities. These parties are now subject to the Entity List FDP Rule that restricts the entities' ability to obtain foreign-produced chips and other items. BIS added additional PRC entities under this FDP Rule in December 2022. Much of the rationale for the advanced computing changes also applies to the new controls related to semiconductor manufacturing. Advanced semiconductors are key to developing advanced weapon systems, exascale supercomputing capabilities, and AI capabilities.

With respect to semiconductor manufacturing, the October 7, 2022, rule made three main changes. First, BIS implemented new PRC-wide restrictions on exports of certain manufacturing tools essential for high-end chip production, regardless of the end user. Next, BIS also imposed restrictions on the export of any U.S. tools or components to a PRC semiconductor fabrication facility that is capable of advanced logic or memory chip production. For these advanced fabrication facilities, we also imposed a license requirement on U.S. persons providing support to those entities. Finally, we imposed controls on items that will be used to develop or produce indigenous semiconductor manufacturing equipment in the PRC.

These changes, as well as the October 2023 updates, are designed to address concerns related to the production of advanced semiconductors. These controls are not

intended to stop production of legacy semiconductors, and these controls are not tools of economic protectionism. They are national security and foreign policy tools.

41. What actions is the BIS taking to refine the advanced computing rule, and how does the agency ensure that its measures are as effective as possible to protect U.S. national security?

Since the rule's announcement on October 7, 2022, BIS has taken a number of steps to ensure its effectiveness. This includes extending a public comment period, issuing related FAQs, and engaging closely with international partners in coordinating approaches to export controls of these and other items to the PRC. In the intervening months, key international supplier governments have independently and publicly released information related to new restrictions they intend to put in place through their domestic legal systems to restrict the export of advanced semiconductor manufacturing equipment. On October 17, 2023, BIS issued additional rules that account for public comments received since publication of the October 2022 rule, as well as additional analysis and information from federal agency partners. Additional information about the important updates made to the October 2022 rule by the rules issued on October 2023 is available on BIS's website here: https://www.bis.doc.gov/index.php/policy-guidance/advanced-computing-and-semiconductor-manufacturing-items-controls-to-prc.

The Department understands that export controls must stay ahead of an evolving threat environment, which is why we are constantly and relentlessly vigilant, in coordination with our interagency partners, in reviewing available classified and open-source information, to enforce and appropriately update our export controls to address the threats posed by the PRC. The October 17, 2023, rules outline multiple issues on which BIS soughtadditional public comment, and as appropriate, the Department will make additional adjustments to our controls in response to public comments and other factors.

42. How does the BIS gather specific and articulable evidence to add foreign entities that pose a threat to U.S. national security or foreign policy to the Entity List, and what

authorization requirements are imposed on U.S. technology shipments to these entities?

The Entity List (supplement no. 4 to part 744 of the Export Administration Regulations) identifies entities for which there is reasonable cause to believe, based on specific and articulable facts, that the entities—including businesses, research institutions, government and private organizations, individuals, and other types of legal persons—that have been involved, are involved, or pose a significant risk of being or becoming involved in activities contrary to the national security or foreign policy interests of the United States. Parties on the Entity List are subject to individual licensing requirements and policies supplemental to those found elsewhere in the EAR.

BIS utilizes available open-source, proprietary, and classified information in coordination with the Intelligence Community as well as the U.S. and international law enforcement community to assess potential entities of concern.

Entity List additions are determined by the interagency End-User Review Committee (ERC) comprised of the Departments of Commerce (Chair), Defense, State, Energy, and where appropriate, the Treasury. The ERC makes decisions regarding additions to add an entity to the Entity List by majority vote and makes all decisions to remove or modify an entity by unanimous vote.

43. What are the criteria and considerations behind adding China parties to the BIS Entity List, and how has the number of China-related entities on the list changed during the current administration?

BIS adds entities to the Entity List upon a determination that that there is reasonable cause to believe based on specific and articulable facts, that an entity has been involved, or poses a significant risk of being or becoming involved in, activities that are contrary to the national security or foreign policy interests of the United States. In consultation with our interagency partners at the Departments of State, Defense, and Energy, we diligently ensure entities added to the Entity List meet that standard.

The Entity List, as well as other restricted parties' lists (i.e., the Denied Persons List and the Military End User List) currently encompass more than 2,000 entities

through approximately 2,900 entries (i.e., affiliates, subsidiaries, etc., sometimes located in multiple countries), in approximately 80 countries.

Under the Biden Administration, the Entity List has been an important tool for protecting U.S. national security and foreign policy interests, as evidenced by the fact that more entries were added in 2023 than in any other year of the Entity List's existence. While a high number of total listings is not necessarily an objective of BIS, the Entity List is a powerful tool that is both flexible and targeted and can be employed quickly based on unique circumstances, as evidenced by numerous Russia- and related actions, and the restrictions imposed by BIS on the People's Liberation Army's (PLA) aerospace programs including airships and balloons and related materials and components. Expanded use of the Entity List also has the benefit of being well understood by industry and foreign partners, and the clear processes and standards demonstrate U.S. commitment to the rule of law.

BIS has undertaken significant Entity List actions against the PRC or PRC-related entities for their support of the PRC's military actors and military modernization efforts, support of the PRC's weapons of mass destruction programs, and for enabling or engaging in human rights abuses. The over 300 entities added during this Administration make up nearly 40 percent of all PRC entities added since the creation of the list and demonstrate the serious and sustained focus by the Administration on entities within the PRC engaged in activities contrary to U.S. national security and foreign policy interests. It is also worth noting that the approach taken by this Administration is deliberate, targeted, and focused on particular entities of concern and builds on the work done in prior Administrations that identified significant large PRC firms of concern, such as Huawei, and added over 150 Huawei affiliates and subsidiaries, which illustrates further that focusing solely on the number of entities or entries added to the Entity List is not necessarily the most effective metric for determining the national security and foreign policy impact of Entity List actions.

In addition to addressing the national security and foreign policy threats related to the PRC, BIS has simultaneously taken a series of actions against the Russian Federation (Russia) for its brutal invasion of Ukraine undertaken with the complicity of Belarus. As of December 7, 2023, over 800 entities located in Russia and third countries have been added to the Entity List for acquiring or attempting to acquire items subject to the EAR in support of Russia's military, or for other reasons related to Russia's invasion of Ukraine, including support of Russia's defense and security sectors.

BIS continues to add entities for other acts that are contrary to U.S national security and foreign policy interests, such as engaging in cyber exploits that threaten the privacy and security of individuals and organizations worldwide, enhancing the military capabilities of adversaries, or preventing BIS from performing end use checks.

44. How important are global partners in the effectiveness of export controls? How does the BIS collaborate with international export control coalitions to achieve common approaches to issues of common concern?

As outlined in the Export Control Reform Act (ECRA), multilateral controls are more effective than unilateral controls. BIS regularly consults with foreign governments on export control matters, including within the four multilateral export control regimes and on a bilateral basis. As Congress noted in ECRA, "[e]xport controls that are multilateral are most effective[.]" If other countries supply the same types of items that the United States restricts, the U.S. controls will be less effective for two reasons. First, the countries or parties of concern will still acquire the items at issue. Second, U.S. technology leadership will be threatened if foreign competitors can undercut U.S. companies and earn revenue to invest in research and development. Thus, coordinating with allies and partners helps keep a level playing field for U.S. companies and helps to maintain U.S. technology leadership and competitiveness, all of which contribute to national security, as described in ECRA.

A clear example of this is the effectiveness of the nearly 40 international allies and partners that have joined us in implementing substantially similar controls, which have restricted Russia's ability to obtain key commodities and technologies. Over time, we are starving Russia's military industrial base and limiting their ability to repair, replace, and replenish their most advanced weapons and platforms. These measures and the financial sector sanctions imposed by the Treasury Department, along with the robust military, financial, diplomatic and other support provided by the Administration and our international allies and partners enhance Ukraine's ability to counter Russian aggression.

However, as demonstrated by BIS's unilateral action to issue its October 7, 2022, rules to restrict the PRC's access to advanced computing and semiconductor manufacturing, the U.S. reserves the right to act when our national security interests

require it. We continue to engage with international partners and allies to bring them on board and implement substantially similar controls, and since issuance of the 2022 controls some have done so.

The Department has established the Quad Critical and Emerging Technologies working group with Japan, Australia, and India, as well as participating in the U.S.-EU Trade and Technology Council, or TTC, which are working to align our approaches in order to secure supply chains, export controls, data governance, and investment screening. We are witnessing the strength of this partnership in the extraordinary degree of coordination we have achieved around the implementation of export controls against Russia in response to its 2022 invasion of Ukraine.

45. How does the BIS ensure that export controls evenly affect all relevant industries around the world, and what measures are taken to prevent loopholes or inconsistent enforcement?

BIS is in constant communication with international allies and partners that share our democratic values, security, and other interests to help them understand our views on the current threat environment, explain our approach to export controls, and to enlist their assistance in aligning controls.

46. How does the BIS assess risk concerning the misuse of technology or the reliability of companies? How are these assessments shared with allies and partners to develop common approaches?

BIS and our interagency partners, particularly at State, Defense, and Energy, but in concert with other agencies as appropriate and with support from the intelligence community, assess all-source information when developing, implementing, and enforcing export controls.

In addition, license applicants are required under the EAR to conduct substantial due diligence into their customers ("Know your customer" requirements), particularly in the PRC given the potential for diversion. Failure to do so exposes exporters to

potential administrative and civil penalties, including fines, revocation of export privileges, and, in conjunction with the Justice Department, criminal penalties.

The United States is also in constant communication with allies and partners to develop new controls through the four existing multilateral regimes (Wassenaar Arrangement, Missile Technology Control Regime, Australia Group (chemical/biological issues), and the Nuclear Suppliers Group), as well as in other contexts such as the U.S.-EU Trade and Technology Council and Global Export Control Coalition (GECC). The GECC is made up of the United States and 38 partner governments and we have greatly enhanced our information sharing with trusted partners through this coalition, including information on licenses, among other things. While the GECC is focused on addressing Russia's illegal invasion of Ukraine, many of our partners in that effort are also partners in other regimes and share our national security interests and perspectives.

47. What are the challenges and considerations in balancing export controls to counter China's military modernization while preserving U.S. technological leadership and maintaining commercial trade that doesn't undermine U.S. national security?

As outlined in the ECRA, export controls are generally most effective when applied on a multilateral basis, and the United States works to coordinate controls with allies and partners whenever possible. Failing to do so may ultimately undermine U.S. national security by allowing malign actors access to comparable foreign produced goods, putting U.S. industry at a disadvantage while failing to stop those actors from obtaining the items they seek. As a result, the United States has worked vigorously to communicate our national security interests to our international allies and partners and seek their support.

However, it is important to remember that U.S. national security interests come first, and the United States reserves the right to act unilaterally when appropriate. For example, the export controls on advanced semiconductors and semiconductor manufacturing equipment issued on October 7, 2022, were initially implemented on a unilateral basis. Over time, certain other governments independently imposed similar

controls for similar national security reasons on a variety of items, and the United States is very supportive of those decisions and will continue working to communicate, coordinate, and whenever possible, act in concert with allies and partners to enhance U.S., regional, and global security interests.

48. What mechanisms are in place to monitor and evaluate the effectiveness of BIS export controls on China's efforts to obtain sensitive technology and advance its military capabilities?

The United States government utilizes all-source information to monitor and assess the effectiveness of export controls and to aid in our enforcement efforts. This includes public reporting, proprietary data and information, as well as classified information. In addition, BIS executes physical End Use Checks, which are intensive site visits by specially trained Export Control Officers stationed with U.S. Embassy staff abroad, including in the PRC, to verify the bona fides (i.e., legitimacy and reliability) of various parties seeking to receive exports. BIS and our interagency and international partners are in constant communication and constant assessment of the evolving national security context, technology landscape, and commercial environment and do not hesitate to use our regulatory and enforcement tools to protect U.S. national security interests.

49. How does the BIS coordinate with other U.S. government agencies and stakeholders to develop comprehensive strategies that address China's national security threats effectively?

BIS and our interagency partners, particularly at State, Defense, and Energy, but in concert with other agencies as appropriate and with support from the intelligence community, assess all-source information when developing, implementing, and enforcing export controls.

BIS is continually assessing new technologies, in concert with our interagency partners, in order to determine if new controls are appropriate to protect U.S. national

security, achieve U.S. foreign policy objectives, and advance U.S. technological leadership and we will continue to develop and make recommendations for multilateral control of new technologies to the appropriate multilateral regimes as appropriate.

50. What role does technology collaboration and research partnerships play in addressing the challenges posed by China's military civil fusion strategy and technological advancements?

Robust technology collaboration and research partnerships, particularly among trusted partners and allies, are essential to advancing U.S. technological leadership. Collaboration is also essential for advancements that translate not only into national security advantages, but also broad based economic opportunities that raise living standards across the globe, reinforce the benefits of the rules-based international order and democratic values, and that strengthen our hand diplomatically while also undergirding the power of our military.

To encourage this robust collaboration while addressing the challenges posed by military-civil fusion, it is imperative to conduct outreach to foreign governments, foreign industry, and academia to raise awareness regarding targeted technologies under the MCF strategy and to provide tools to prevent the research ecosystem from being exploited by the PRC to advance this strategy.

51. How does the BIS address potential risks of technology diversion or leakage to China through third-party countries or intermediaries?

U.S. technological and economic leadership globally give us tremendous reach and influence into commerce, particularly in advanced items and technologies that have both civilian and military applications.

On the front end, BIS and our interagency partners review license applications thoroughly. BIS's regulations apply to items exported from the United States, reexported from one destination to another, as well as the transfer in-country of items that are subject to the EAR. In other words, the law follows the item, and for items

subject to the EAR, when exporters seek a license from BIS they must identify their supply chain, end users, and other relevant information which is then reviewed by the Departments of Commerce, State, Defense, and Energy.

Before and after a license is approved, BIS may also conduct pre-shipment verifications, or post-license checks, to ensure that items—even those shipped abroad—are appropriately being obtained pursuant to their authorization. While these tools are important, BIS also works very closely with our interagency and international law enforcement colleagues to leverage all source information as appropriate to identify and disrupt illicit networks. If items are found to be diverted, the exporter may be subject to administrative, civil, or criminal penalties.

52. Has the BIS has successfully prevented sensitive U.S. technologies from reaching China's military or entities of concern through export controls? If so, which technologies and how?

Please see response to question 41.

52. How does the BIS engage with the private sector, academia, and industry stakeholders to identify and address potential vulnerabilities in the export control system?

BIS interacts with technology developers and stakeholders such as academia (universities and research institutions), private industry, government, and private research laboratories, as well as science and technology organizations and associations. Through its own technical personnel, technical advisory committees, and interagency working groups, BIS seeks to determine whether there are specific technologies that are essential to the national security of the United States for which effective controls can be implemented that do not adversely impact U.S. leadership in the science, technology, engineering, and manufacturing sectors. BIS also uses these forums to understand business and academia's standard practices and trade flows in order to implement controls that will effectively protect the United States' national security and foreign policy interests while not unnecessarily impeding trade.

53. What steps is the BIS taking to mitigate any potential backlash or retaliatory actions from China in response to export control measures imposed by the U.S.?

BIS works to carefully tailor, and clearly communicate the rationale for, export controls so that other governments—including the PRC—understand the national security interests being addressed by our actions in an effort to limit misunderstandings. BIS makes clear that U.S. national security is not up for negotiation.

The Department is in constant communication with interagency and international partners and as appropriate will be prepared to respond to any retaliatory measures.

54. How does the BIS incorporate emerging technologies, such as quantum computing and artificial intelligence, into its export control framework to address evolving security challenges?

Section 1758 of the Export Control Reform Act directed the President to establish, "a regular, ongoing interagency process to identify emerging and foundational technologies that--(A) are essential to the national security of the United States; and (B) are not critical technologies, " (Critical technologies are those technologies described Section 721(a)(6)(A) of the Defense Production Act of 1950, as amended, such as items on the Commerce Control List controlled pursuant to a multilateral regime and defense articles on the U.S. Munitions List).

On May 23, 2022, BIS informed the public that in future regulatory actions, controls pursuant to section 1758 would be referred to as "section 1758 technologies" rather than as "emerging technology" or "foundational technology." See 87 Fed. Reg. 31195 (May 23, 2022). As noted in the May 23 rule, this approach reflects that, in the absence of statutory definitions and challenges in drawing meaningful and functional distinctions between those terms, it was nevertheless important to implement agreed-upon controls for technologies identified pursuant to section 1758. For example, the marine toxins identified in the May 23 rule defy common attempts to characterize them as "emerging" or "foundational" as these toxins are naturally occurring items that are

not new. However, new synthesis and collection techniques for these toxins have resulted in the need to propose controls on the toxins.

Characterizing these technologies as section 1758 technologies furthers the government's flexibility to respond to real-time developments in rapidly changing technological landscapes and minimize delays in implementing necessary controls. Also, all potential section 1758 technologies will continue to go through the required notice and comment procedure and will be subject to the same minimum controls. This approach will enhance BIS's effectiveness and flexibility to assess and apply appropriate controls to a technology that is essential to the national security of the United States, regardless of whether it is labeled "emerging" or "foundational."

Identifying section 1758 technologies is a continuous, rigorous review process across and throughout vast technology categories and fields. Accordingly, BIS interacts with technology developers and stakeholders such as academia (universities and research institutions), private industry, government, and private research laboratories, as well as science and technology organizations and associations. Through its own technical personnel, technical advisory committees, and interagency working groups, BIS seeks to determine whether there are specific emerging and foundational technologies that are essential to the national security of the United States for which effective controls can be implemented that will not adversely impact U.S. leadership in the science, technology, engineering, and manufacturing sectors.

In addition to these measures, BIS expends considerable time in identifying emerging and foundational technologies through confidential technical information gathering, discussions with technology developers, technical interagency meetings based on public and classified information, and engagements with the BIS Emerging Technology Technical Advisory Committee (ETTAC) and CFIUS.

Consistent with the statutory criteria outlined in section 1758(a)(2)(B) of ECRA, in identifying section 1758 technologies, BIS's process considers the:

1. Development of emerging and foundational technologies in foreign countries;

2. Effect export controls may have on the development of such technologies in the United States; and

3. Effectiveness of export controls on limiting the proliferation of emerging and foundational technologies in foreign countries of concern.

55. How does the BIS assess the dual-use nature of certain technologies and determine their appropriate export control classification in the context of U.S.-China strategic competition? How do those considerations differ in the context of U.S. strategic competition with other countries?

Please see responses to questions 38, 39, and 41.

56. What measures are in place to ensure that the BIS export control policies and strategies align with broader U.S. foreign policy objectives and international security interests?

BIS is in constant communication with international allies and partners that share our democratic values, security, and other interests to help them understand our views on the current threat environment, explain our approach to export controls, and to enlist their assistance in aligning controls.

57. **How does the BIS address the challenge of tracking and controlling the transfer of sensitive technology through online platforms and digital channels?**

BIS imposes license requirements on releases of certain software source code and technology to foreign persons in the United States (a "deemed export"), depending on a variety of case-specific circumstances. In addition, BIS requires licenses for the export, reexport, and transfer (in-country) of certain software and other sensitive technology abroad, including technologies that may be used for surveillance or other activities of concern. In certain circumstances, BIS also requires a disclosure of the transfer of software and technology with encryption capabilities on a periodic basis.

58. How does the BIS approach cases involving Chinese companies or entities with ties to both civilian and military sectors, and what factors are considered in determining the appropriate export control measures?

As National Security Advisor Jake Sullivan noted in a September 2022 speech, the strategic environment we are in today necessitates a new approach on export controls— particularly on technologies that are absolutely critical to national security such as advanced logic and memory chips. For those technologies, we must move away from our previous approach of maintaining "relative" advantages over competitors, and instead seek to prevent them from obtaining certain absolute levels of capability that pose national security risks.

BIS has also acted to impose new controls on critical enabling technologies such as advanced semiconductor manufacturing equipment, high performance chips, and related items, and to vigorously use its regulatory and enforcement authorities including the Entity List to counter the PRC's Military-Civil Fusion program by denying access to the most advanced technologies.

For instance, on June 12, 2023, BIS added 31 entities in the PRC to the Entity List, including 9 entities for acquiring and attempting to acquire U.S.-origin items in support of China's military modernization. Currently, nearly 800 entities in the PRC are listed on the Entity List, restricting their access to items subject to BIS's regulatory jurisdiction. Over 300 of these entities have been added during the Biden-Harris Administration.

59. How does the BIS plan to adapt its export control strategies in response to future technological advancements and potential shifts in China's national security strategies?

BIS will continue to evaluate the threat environment, technological advancements in a variety of industries and sectors, and other factors and will update controls as appropriate to protect U.S. national security and foreign policy interests, as evidenced by the controls announced on October 7, 2022 and October 17, 2023, that seek to address concerns posed by the PRC's efforts to develop high performance computing capacity to train AI and related data and communications technologies that can be

employed for military modernization and human rights abuses. Our restrictions related to advanced semiconductor manufacturing equipment, high performance chips and related items, and other measures outlined in those rules restrict the PRC's ability to obtain the tools and capabilities they desire for these activities and represent an expansion of our controls based on the present threat environment.

60. Is it possible that a PRC company's investment in a U.S. company that produces critical or emerging technologies, but is not subject to export controls or restrictions, could harm the national security of the United States?

The United States has investment screening policies in place to help address such concerns. These authorities are administered by the U.S. Department of the Treasury and are complementary to the export restrictions in place for critical and emerging and foundational technologies.

61. Has the PRC communicated to the Department of Commerce any legitimate justifications for recent restrictions imposed on Micron in the PRC? If so, what were these?

There is an ahistorical quality to some commentary on the PRC's recent actions against Micron, suggesting that these actions are simply a response to recent U.S. export controls. But the story does not begin with this administration's semiconductor export controls or even the previous administration's actions against Huawei.

In fact, the PRC has for many decades pursued state-directed predatory industrial targeting of key sectors implemented by a broad and evolving range of non-market policies and practices, including intellectual property theft, forced technology transfer, massive state support, and discriminatory regulation--all designed to enable

the PRC to not only undercut global competitors but drive them out of the marketplace. We have seen the PRC do this in a wide range of industries, from EV batteries to solar to telecommunications.

The PRC has pursued the same strategy in semiconductors for nearly two decades, with blanket subsidies across its entire industry, coupled with forced technology transfer, regulatory pressure, and blatant IP theft, such as that by Fujian Jinhua, a PRC state-owned memory chipmaker that was placed on the U.S. Entity List for IP theft. A Reuters investigation found that PRC actions targeting Micron have been going on for several years, including the state directing domestic demand to domestic firms including Huawei and Inspur.

The Department is working closely with our allies and partners to counter the use of coercive economic practices broadly. BIS will also continue working to prevent malign actors from obtaining or diverting technologies that can be used against the United States or its allies in order to protect our national security and advance our foreign policy objectives. Should national security concerns exist, we will not hesitate to vigorously use our tools to address the threat as appropriate.

62. What has the Department of Commerce done to support Micron in response to PRC restrictions imposed in May and deter similar attempts at economic coercion against United States companies?

See response to question 61.

63. Could PRC domination and control of lagging or commoditized semiconductor production threaten United States national security or undermine U.S. companies?

On January 18, 2024, BIS released an industrial base survey, conducted pursuant to BIS's Defense Production Act authorities, into mature node semiconductors. Secretary Raimondo stated, "Legacy chips are essential to supporting critical U.S. industries, like telecommunications, automotive and the defense industrial base.

Addressing non-market actions by foreign governments that threaten the U.S. legacy chip supply chain is a matter of national security. Over the last few years, we've seen potential signs of concerning practices from the PRC to expand their firms' legacy chip production and make it harder for U.S. companies to compete. To get ahead of these concerns, the Department of Commerce is taking proactive measures to assess the U.S. semiconductor supply chain by collecting data from U.S. companies on the sourcing of their legacy chips. Government alone cannot create and sustain a robust supply chain—we need industry at the table. This survey will empower the Department with the data we need to inform our next steps in building strong, diverse, and resilient semiconductor supply chains."

The intent of the survey is to identify how U.S. companies are sourcing mature-node semiconductors, also known as legacy chips. This analysis will inform U.S. policy to bolster the semiconductor supply chain, promote a level playing field for legacy chip production, and reduce national security risks posed by the People's Republic of China (PRC).

The assessment was requested by the Secretary of Commerce in response to findings in a Congressionally mandated report released in December 2023 that assessed the capabilities of the U.S. microelectronics industrial base to support U.S. national defense. The findings of that report, titled "Assessments of the Status of the Microelectronics Industrial Base in the United States," are available online at: https://www.bis.doc.gov/index.php/other-areas/office-oftechnology-evaluation-ote/industrial-base-assessments

The survey will be performed under Section 705 of the Defense Production Act of 1950 to evaluate the extent of, and visibility into, the use of mature-node chips manufactured by PRC-based companies in supply chains of critical U.S. industries like telecommunications, automotive, medical device, and the defense industrial base.

More information on the survey is available online at: https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3437-2024-01-18-bis-press-release-legacy-chip-survey-final/file.

64. Does the rise of COMAC threaten U.S. economic security?

The United States is home to a robust aerospace industry that produces world-class aircraft and related technology. The Department of Commerce is committed to supporting the continued vitality and innovation of that critical sector to ensure that American companies can continue to outcompete any international competitors. This includes through careful review of export licenses for relevant items under BIS's jurisdiction to protect sensitive U.S. technologies, as well as through activities to promote American aerospace through the International Trade Administration and others.

65. What tools have the administration considered using to reduce the trade deficit with China?

The Administration is working to protect U.S. national and economic security interests while also taking steps to address the unfair and unbalanced trade relationship with the PRC. The PRC is our third largest trading partner, receiving over $147 billion in goods exports alone in 2023, and U.S. exports help support and create high-paying U.S. jobs. Increased exports to the PRC in non-sensitive sectors can help U.S. firms and workers without harming U.S. national security.

While the PRC market holds great opportunities for U.S. exporters, there are still numerous non-tariff barriers to trade that still need to be addressed. Secretary Raimondo highlighted this issue during her visit to China last August, calling on the PRC government to match their rhetoric with action if they want U.S. companies to do business in China. The PRC needs to live up to its commitments and take meaningful steps to create an open and level playing field for foreign businesses, including ensuring a fair and transparent regulatory environment and effective protection of intellectual property. The Commerce Department is working to address trade barriers faced by U.S. companies as well as supporting U.S. exports in non-sensitive sectors through trade promotion activities.

66. What steps has the Administration take, or plan to take, to return steel and aluminum processing and/or manufacturing to the United States?

To outcompete the PRC, we need bold domestic investments and innovation ecosystems that bring manufacturing in critical technologies and industries back to the United States. Without manufacturing strength in the United States and the innovation that flows from it, we risk falling behind the PRC in the race to invent and commercialize future generations of technology. Diverse, resilient, and sustainable supply chains are critical for national security and economic competitiveness, and a key element of this effort is revitalizing domestic manufacturing, reducing our reliance on the PRC, and positioning ourselves to be proactive instead of reactive.

In the first two years of the Biden-Harris Administration, the Commerce Department worked with Congress to enact the American Rescue Plan, the Bipartisan Infrastructure Law, the CHIPS and Science Act, and the Inflation Reduction Act. Taken together, they represent historic investments in America and a once-in-a-generation commitment to advancing innovation, technology, manufacturing, workforce training, supply chain resilience, and the infrastructure that we need to ensure our future competitiveness and national security. These investments drive innovation, job creation, and economic growth that strengthen our position to outcompete the PRC, and their effectiveness would be threatened by repealing or under-resourcing the laws enacted by Congress.

In addition to the investments under those laws, as you are likely aware, the Commerce Department initiated Section 232 Investigations into imports of steel and aluminum products in 2017. These Investigations found that the high quantities of such imports and the circumstances of global excess capacity in steel and aluminum were weakening domestic production capacity for such products and thereby threatening to impair the national security as defined in Section 232 of the Trade Expansion Act of 1962.

The Secretary of Commerce thus developed a global tariff on imports of steel and aluminum articles under Section 232 to reduce imports to a level that would enable domestic steel producers to achieve and sustain the use of roughly eighty percent of existing domestic production capacity and thereby achieve long-term economic viability through increased production in the United States.

The Department of Commerce still sees the tariffs on steel and aluminum under Section 232 as playing a key role in upholding the national security of the United States.

Since the imposition of the tariffs in March 2018, Commerce has observed an overall decrease in imports and increase in domestic production of steel and aluminum, with corresponding gains in the usage of domestic production capacity. China has reportedly begun curbing its annual steel production, but the circumstances of excess global capacity remain acute and continue to reinforce the need for the actions taken under Section 232.

67. Does the PLA use supercomputers designed or built by Inspur? Does the PLA use supercomputers designed or built by any Inspur subsidiaries or joint ventures?

The Department would refer the Committee to the intelligence community for information responsive to this question.

68. Does the PLA use supercomputers designed or built by Lenovo? Does the PLA use supercomputers designed or built by any Lenovo subsidiaries or joint ventures?

The Department would refer the Committee to the intelligence community for information responsive to this question.

69. Does the Department of Commerce believe U.S. technology should go to firms that build supercomputers in the PRC, like Inspur?

In March 2023, Inspur Group was added to the Entity List for acquiring and attempting to acquire U.S.-origin items in support of China's military modernization efforts. The Department and its interagency colleagues remain vigilant in addressing concerns related to firms that may be supporting the PRC's military modernization and will not hesitate to take action as appropriate to protect U.S. national security and foreign policy interests, as evidenced by the powerful PRC-wide export controls on advanced semiconductors and semiconductor manufacturing equipment put in place in October 2022 and updated and expanded in October 2023, and through vigorous use of

the Entity List. Under the Biden Administration over 1,100 entities (Over 40 percent of all entities) have been added to the Entity List, including over 300 in the PRC.

70. What is the Department of Commerce's plan to close the subsidiary loophole whereby Inspur has bypassed U.S. export control through its subsidiaries?

In March 2023, the Inspur Group was added to the Entity List for acquiring and attempting to acquire U.S.-origin items in support of the PRC's military modernization efforts. As outlined in longstanding FAQs, Entity Listing is a "red flag" and U.S. exporters seeking to conduct business with entities affiliated with Entity Listed entities should conduct careful due diligence prior to proceeding with transactions. BIS stands ready to assist exporters with any questions related to such transactions. BIS regularly assesses available open-source, proprietary, and classified information in coordination with the Intelligence Community as well as the U.S. and international law enforcement community to assess potential entities of concern for potential addition to the Entity List.

In addition, it is important to note that BIS has instituted PRC-wide restrictions on advanced semiconductors, semiconductor manufacturing equipment, and related items under its October 2022 and 2023 rules. These restrictions impose license requirements on transactions with entities—regardless of their placement on the Entity List or not—in the PRC for items subject to the rules. These carefully crafted restrictions seek to limit the PRC's ability to obtain the items necessary to support the PRC's indigenous development of items necessary to produce advanced artificial intelligence, supercomputing capacity, and other applications that support the PRC's military modernization. These restrictions apply to Inspur group as well as any affiliates and subsidiaries.

71. How many export control licenses has the Department of Commerce approved to Inspur since April 2023?

This information is protected from general disclosure under section 1761(h) of ECRA. The Committee may seek this information pursuant to that provision.

72. Has the Department of Commerce ever refused to submit any State-Department nominated PRC entity to the ERC?

The Commerce Department does not comment on interagency deliberations. Under the Export Administration Regulations (EAR), all additions to the Entity List require a majority vote of the End-User Review Committee (ERC), which is chaired by Commerce, with representatives from the Departments of State, Defense, Energy, and where appropriate, the Treasury. For each entity on the Entity List, the ERC determines, based on specific and articulable facts, whether the entity has been involved in, is involved in, or poses a significant risk of being or becoming involved in activities that are contrary to the national security or foreign policy interests of the United States.

73. Did the Department of Commerce attempt to nominate YMTC to the Entity List in October 2022?

YMTC was added to the Entity List effective December 16, 2022 (See 87 Fed. Reg. 77505 (Dec. 19, 2022)) on the basis of information indicating that the company presents a risk of diversion to parties on the Entity List: https://www.federalregister.gov/documents/2022/12/19/2022-27151/additions-and-revisions-to-the-entity-list-and-conforming-removal-from-the-unverified-list

74. Did the Department of Commerce have to rely on the State Department to nominate the PRC entities affiliated with the spy balloon?

The Commerce Department does not comment on interagency deliberations. The End-User Review Committee, made up of the Departments of Commerce, State, Defense, and Energy, makes all decisions regarding additions, modifications, and removals to the Entity List. In general, any member of the ERC can initiate an evaluation of a potential party of concern for potential addition to the Entity List. The Department of Commerce issued a rule, effective on February 10, 2023, adding several entities based in the PRC to the Entity List for activities contrary to U.S. national security and foreign policy interests. These entities were added for their support to

China's military modernization efforts, specifically the People's Liberation Army's (PLA) aerospace programs including airships and balloons and related materials and components. https://www.federalregister.gov/documents/2023/02/14/2023-03193/additions-to-the-entity-list See 88 Fed. Reg. 9389 (Feb. 14, 2023).

75. Does the Department of Commerce believe the allowed transfer rate standard established in the October 7 export controls should be reduced?

On October 17, 2023, BIS issued three rules making modifications to the restrictions on advanced semiconductors and semiconductor manufacturing equipment issued in October 2022.

Specifically related to the parameters established under the October 2022 rule, the Advanced Computing/Supercomputing Interim Final Rule (AC/S IFR) issued on October 17, 2023, retains the licensing requirements for the PRC (including Hong Kong and Macau) imposed in the October 7, 2022, rule and makes several updates:

- Adjusting the parameters that determine whether an advanced computing chip requires a license; and
- Imposing new measures to address risks of circumvention of the controls including by expanding controls to additional countries.

Parameter Changes:

Based on public comments, recent technological developments, and analysis of the prior rule's national security impact, the AC/S IFR removes "interconnect bandwidth" as a parameter for identifying restricted chips. The rule also:

- Restricts the export of chips if they exceed either of two parameters:

(1) The performance threshold set in the October 7 rule; or

(2) A new "performance density threshold," which is designed to preempt future workarounds.

Additional information on the changes made in the AC/S IFR and other rules issued on October 17, 2023 is available at: Advanced Computing and Semiconductor Manufacturing Items Controls to PRC (doc.gov)

76. Does the Department of Commerce have a plan to deal with the expansion of PRC cloud computing providers globally?

Among other changes, the October 17, 2023, Advanced Computing/Supercomputing Interim Final Rule (AC/S IFR) rule expanded end-use controls that are needed to ensure that the national security objectives of the October 2022 and updated October 2023 rules are not undermined by Macau, PRC, or other Country Group D:5 entities setting up cloud or data servers in other countries that allow these headquartered companies of concern to continue to train their AI models in ways that would be contrary to U.S. national security interests. The expanded end-use controls are intended to target entities of concern, such as a PRC-headquartered cloud or data server provider located outside of China in a destination other than Country Groups D:1, D:4, or D:5, excluding any destination also specified in Country Groups A:5 or A:6. The license requirements under this end-use control apply to destinations in Country Group A:5 and A:6 and any other destination not specified in Country Groups D:1, D:4, or D:5.

These changes will provide greater visibility into the use of these advanced computing chips, which will enhance compliance monitoring and enforcement. The rule also requested public comments on multiple topics, including risks associated with infrastructure as a service (IaaS) providers. Additional information on the rules issued on October 17, 2023 are available at: Advanced Computing and Semiconductor Manufacturing Items Controls to PRC (doc.gov)

In addition to the controls put in place in October 2022 and 2023, BIS also maintains controls on other key enabling technologies and certain end users that present U.S. national security or foreign policy concerns. In addition to semiconductors and related items, BIS maintains controls on encryption technology found in Category 5, Part 2, as well as ubiquitous hardware components that include: Graphics processing units (GPUs), Neural Network accelerators, central processing units (CPU), application specific integrated circuits (ASIC) units, or cloud computing technology. Restrictions

also apply to certain inputs—software and IP-libraries, certain types of data—that are necessary for the production of such items. In other words, AI applications incorporated into software, technology, or equipment subject to the EAR may be subject to license requirements if the software incorporates encryption, or if it is necessary for the development, production, use, operation, installation, maintenance, or repair of a licensable item.

Restrictions on items for export to the PRC or specified end users in the PRC include items necessary for the development of cloud computing systems within the PRC. As a result, PRC entities are subject to restrictions when it comes to obtaining certain items necessary for developing their own cloud computing capacity. In addition, BIS maintains a series of tools and restrictions that can be employed when particular entities are found to be engaging in activities contrary to U.S. national security or foreign policy interests.

Furthermore, EO 13873, "Securing the Information and Communications Technology and Services Supply Chain," (May 15, 2019) authorized the Secretary of Commerce to prohibit or impose mitigation measures on any ICTS Transactions subject to United States jurisdiction that pose undue or unacceptable risks to the United States. The regulations implementing the EO (see 15 C.F.R. Part 7) establish what constitutes an ICTS Transaction and create a process for reviewing ICTS Transactions the Department or other agencies (through referrals) believe may pose undue or unacceptable risks. Further, the Department can investigate ICTS Transaction on its own accord or upon referral from another agency. Ultimately, the Secretary can prohibit or mitigate ICTS Transactions if those transactions are determined to meet the standard articulated in EO 13873. The PRC is listed on the foreign adversary list within EO 13873.

Finally, on January 29, 2024, the Department of Commerce (Department) published a notice of proposed rulemaking (NPRM) for establishing new requirements for Infrastructure as a Service providers (IaaS or "cloud infrastructure providers"). The NPRM outlines proposed requirements to address the risk of foreign malicious actors using U.S. cloud services that could be used in malicious cyber-enabled activity to harm

U.S. critical infrastructure or national security, including to train large artificial intelligence (AI) models. The proposed rule introduces potential regulations that require U.S. cloud infrastructure providers and their foreign resellers to implement and maintain Customer Identification Programs (CIPs), which would include the collection of "Know Your Customer" (KYC) information. Additional information on that proposal is available here: https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3443-2024-01-29-bis-press-release-infrastructure-as-as-service-know-your-customer-nprm-final/file.

77. Does the Department of Commerce believe U.S. cloud providers should be allowed to provide advanced AI training services to PRC entities?

On October 30, 2023, President Biden issued Executive Order 14110, "Safe, Secure, and Trustworthy Use and Development of Artificial Intelligence," which directs the Secretary of Commerce to require foreign resellers of U.S. IaaS products to verify the identity of foreign persons who obtain accounts. The EO further mandates that these cloud providers report to the Department of Commerce when their services are used by foreign nationals, including of the PRC, to conduct a "training run" for a large AI model capable of being used for malicious cyber purposes against the United States. The EO also directs the Secretary to determine the technical definition of a large AI model and sets an interim definition that will be periodically updated, given the rapidly changing nature of the technology.

On January 29, 2024, the Department of Commerce (Department) published a notice of proposed rulemaking (NPRM) for establishing new requirements for Infrastructure as a Service providers (IaaS or "cloud infrastructure providers"). The NPRM outlines proposed requirements to address the risk of foreign malicious actors abusing U.S. cloud infrastructure for malicious cyber-enabled activity to harm U.S. critical infrastructure or national security, including to train large AI models. Additional information on that proposal is available here: https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-

releases/3443-2024-01-29-bis-press-release-infrastructure-as-as-service-know-your-customer-nprm-final/file.

In addition, among other changes, the October 17, 2023, Advanced Computing/Supercomputing Interim Final Rule also expanded end-use controls that are needed to ensure that the national security objectives of the October 2022 and updated October 2023 rules are not undermined by Macau, PRC, or other Country Group D:5 entities setting up cloud or data servers in other countries that allow these headquartered companies of concern to continue to train their AI models in ways that would be contrary to U.S. national security interests. The expanded end-use controls are intended to target entities of concern, such as a PRC-headquartered cloud or data server provider located outside of China in a destination other than Country Groups D:1, D:4, or D:5, excluding any destination also specified in Country Groups A:5 or A:6. The license requirements under this end-use control apply to destinations in Country Group A:5 and A:6 and any other destination not specified in Country Groups D:1, D:4, or D:5.

These changes will provide greater visibility into the use of these advanced computing chips, which will enhance compliance monitoring and enforcement. The rule also requested public comments on multiple topics, including risks associated with IaaS providers. Additional information on the rules issued on October 17, 2023, are available at: https://www.bis.doc.gov/index.php/policy-guidance/advanced-computing-and-semiconductor-manufacturing-items-controls-to-prc.

78. Does the Department of Commerce believe U.S. technology should go into PRC cloud computing centers, globally?

On October 7, 2022, BIS issued a rule imposing PRC-wide restrictions on advanced computing/supercomputing chips, semiconductor production tools, and related items. On October 17, 2023, BIS issued three additional rules updating the 2022 restrictions in a number of ways. Among other changes, the October 17, 2023, Advanced Computing/Supercomputing Interim Final Rule also expanded end-use controls that are needed to ensure that the national security objectives of the October 2022 and updated October 2023 rules are not undermined by Macau, PRC, or other Country Group D:5 entities setting up cloud or data servers in other countries that allow these headquartered companies of concern to continue to train their AI models in ways that would be contrary to U.S. national security interests. The expanded end-use controls are intended to target entities of concern, such as a PRC-headquartered cloud or data server

provider located outside of China in a destination other than Country Groups D:1, D:4, or D:5, excluding any destination also specified in Country Groups A:5 or A:6. The license requirements under this end-use control apply to destinations in Country Group A:5 and A:6 and any other destination not specified in Country Groups D:1, D:4, or D:5.

These changes will provide greater visibility into the use of these advanced computing chips, which will enhance compliance monitoring and enforcement. The rule also requested public comments on multiple topics, including risks associated with IaaS providers. Additional information on the rules issued on October 17, 2023, are available at: Advanced Computing and Semiconductor Manufacturing Items Controls to PRC (doc.gov).

79. Does the Department of Commerce believe Huawei or its technology has been used to spy on the United States?

The intelligence community would be best positioned to provide a response to this question.

80. Does the Department of Commerce believe ZTE or its technology has been used to spy on the United States?

The intelligence community would be best positioned to provide a response to this question.

81. How has the PRC's strategy of "dual-circulation" changed the Department of Commerce's export control policy?

BIS and our interagency partners are constantly monitoring the policies of the PRC and assessing whether appropriate updates to U.S. export controls are necessary to protect U.S. national security and foreign policy interests.

82. Does the Department of Commerce believe U.S. technology should go to PRC firms implicated in human rights abuses?

BIS is actively formulating, coordinating, and implementing various export control measures to counter the use of items subject to our regulations that enable human rights violations and abuses. We have long implemented unilateral controls on items that by their nature are particularly useful to police and security services and could be used for arbitrary detention or arrest, dispersal of peaceful protests, and other activities of human rights concern. This includes items such as: restraints, stun guns, stun grenades, water cannons, saps, police batons, whips, instruments of torture (e.g., thumbscrews), equipment for executions, tear gas, and shot guns, along with related technologies for such items.

BIS also has controls on high tech surveillance items such as surreptitious intercept, key logging, and intrusion equipment and certain biometric items that may be used to enable abusive genetic collection and analysis. These items have a multitude of legitimate end uses but also may be used to engage in or enable human rights violations and abuses. We are keenly focused on appropriately controlling new advanced surveillance tech to inhibit U.S. software and technology from being misused, and to ensure human rights-related export controls reflect the realities of today, with an eye on the future.

Separate from specific items, we consider human rights when reviewing nearly all licensing applications, even where items to be exported are not specifically controlled for human rights-related reasons. All license applications we receive for the export of items, including firearms, are reviewed by BIS foreign policy experts and our international affairs partners at the U.S. Department of State for assessment of foreign policy and human rights implications. We take human rights protection into account when we look at the items, destination, end-users, specific nature of the end use, and the risk of unauthorized use or diversion. Our end-user controls are based on recognition that authoritarian regimes, repressive governments, and complicit commercial entities seek U.S.- origin items to engage in or enable human rights violations and abuses throughout the world. For example, in March 2023, BIS issued a rule (88 Fed. Reg. 18983, Mar. 28, 2023) that added five entities based in the PRC to the Entity List for being implicated in human rights violations and abuses in the

implementation of the PRC's campaign of repression, mass arbitrary detention, and high-technology surveillance against Uyghurs and members of other Muslim minority groups in the Xinjiang Uyghur Autonomous Region (XUAR). This rule also rule reaffirms the protection of human rights worldwide as a U.S. foreign policy interest that is a basis for adding parties to the Entity List.

In addition to our unilateral controls and longstanding multilateral regimes, new arrangements are emerging to leverage export controls to confront threats posed by other misuses of technology, such as by authoritarian regimes to abuse human rights. For example, in March 2023, the United States announced the release of a Code of Conduct for the Export Controls and Human Rights Initiative, as part of the Summit for Democracy, whereby subscribing states, including the United States, Germany, and eleven additional EU countries, take human rights into account when authorizing potential exports and share information on risks associated with the trade of goods, software, and technologies that pose human rights concerns.

83. Does the Department of Commerce believe U.S. technology should go to PRC firms that facilitate transnational repression?

See response to question 82.

84. Does the U.S. Department of Commerce believe U.S. capital should go into the PRC in critical and emerging technologies?

On August 9, 2023, President Biden signed an executive order on "Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern," which states that,

> countries of concern are engaged in comprehensive, long-term strategies that direct, facilitate, or otherwise support advancements in sensitive technologies and products that are critical to such countries' military,

intelligence, surveillance, or cyber-enabled capabilities. Moreover, these countries eliminate barriers between civilian and commercial sectors and military and defense industrial sectors, not just through research and development, but also by acquiring and diverting the world's cutting-edge technologies, for the purposes of achieving military dominance. Rapid advancement in semiconductors and microelectronics, quantum information technologies, and artificial intelligence capabilities by these countries significantly enhances their ability to conduct activities that threaten the national security of the United States. Advancements in sensitive technologies and products in these sectors will accelerate the development of advanced computational capabilities that will enable new applications that pose significant national security risks, such as the development of more sophisticated weapons systems, breaking of cryptographic codes, and other applications that could provide these countries with military advantages.

As part of this strategy of advancing the development of these sensitive technologies and products, countries of concern are exploiting or have the ability to exploit certain United States outbound investments, including certain intangible benefits that often accompany United States investments and that help companies succeed, such as enhanced standing and prominence, managerial assistance, investment and talent networks, market access, and enhanced access to additional financing. The commitment of the United States to open investment is a cornerstone of our economic policy and provides the United States with substantial benefits. Open global capital flows create valuable economic opportunities and promote competitiveness, innovation, and productivity, and the United States supports cross-border investment, where not inconsistent with the protection of United States national security interests. However, certain United States investments may accelerate and increase the success of the development of sensitive technologies and

products in countries that develop them to counter United States and allied capabilities.

The Executive Order directs the Secretary of the Treasury, in consultation with the Secretary of Commerce, and as appropriate, the heads of other relevant executive departments and agencies to issue regulations that require United States persons to provide notification of information relative to certain transactions involving covered foreign persons and that prohibit United States persons from engaging in certain other transactions involving covered foreign persons, among other provisions.

This rulemaking process is ongoing and the Commerce Department looks forward to continuing work with interagency colleagues and stakeholders, including Congress, to implement and execute this new outbound investment security program.

85. Does the U.S. Department of Commerce believe U.S. dependence on the PRC for "legacy" semiconductors represents a supply chain and/or national security risk?

In June 2021, the White House released "Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth," a report compiling the supply chain assessments, recommendations, other findings of several agencies including Commerce as directed under Executive Order 14017.

As the report notes, "The U.S. semiconductor industry accounts for nearly half of global semiconductor revenue, yet the share of semiconductor manufacturing capacity on U.S. soil has fallen from 37 percent 20 years ago and stands at about 12 percent of global production. U.S. companies, including major fabless semiconductor companies, depend on foreign sources for semiconductors, especially in Asia, creating a supply chain risk. Many of the materials, tools, and equipment used in the manufacture of semiconductors are available from limited sources, semiconductor manufacturing is geographically concentrated, and the production of leading-edge semiconductors requires multi-billion dollar investments."

While the supply chain assessments and recommendations identified in that report were developed in response to the supply chain issues presented by COVID-19, the policies and recommendations identified in that report, and the resources and policies subsequently provided by Congress under the CHIPS and Science Act, outline clearly the U.S. strategy for strengthening the resilience of our semiconductor supply chains and promoting continued U.S. technological leadership in this sector.

Further, on January 18, 2024, BIS released an industrial base survey, conducted pursuant to BIS's Defense Production Act authorities, into mature node semiconductors. Secretary Raimondo stated, "Legacy chips are essential to supporting critical U.S. industries, like telecommunications, automotive and the defense industrial base. Addressing non-market actions by foreign governments that threaten the U.S. legacy chip supply chain is a matter of national security. Over the last few years, we've seen potential signs of concerning practices from the PRC to expand their firms' legacy chip production and make it harder for U.S. companies to compete. To get ahead of these concerns, the Department of Commerce is taking proactive measures to assess the U.S. semiconductor supply chain by collecting data from U.S. companies on the sourcing of their legacy chips. Government alone cannot create and sustain a robust supply chain—we need industry at the table. This survey will empower the Department with the data we need to inform our next steps in building strong, diverse, and resilient semiconductor supply chains." More information on the survey is available online at: https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3437-2024-01-18-bis-press-release-legacy-chip-survey-final/file.

86. What is the U.S. Department of Commerce's plan to address the proliferation of PRC legacy semiconductors in the U.S. market?

On January 18, 2024, BIS announced it is conducting a comprehensive assessment of the use of mature-node semiconductor devices in the supply chains that support—directly or indirectly—U.S. national security and critical infrastructure. Secretary Raimondo stated, "Legacy chips are essential to supporting critical U.S. industries, like telecommunications, automotive and the defense industrial base. Addressing non-

market actions by foreign governments that threaten the U.S. legacy chip supply chain is a matter of national security. Over the last few years, we've seen potential signs of concerning practices from the PRC to expand their firms' legacy chip production and make it harder for U.S. companies to compete. To get ahead of these concerns, the Department of Commerce is taking proactive measures to assess the U.S. semiconductor supply chain by collecting data from U.S. companies on the sourcing of their legacy chips. Government alone cannot create and sustain a robust supply chain—we need industry at the table. This survey will empower the Department with the data we need to inform our next steps in building strong, diverse, and resilient semiconductor supply chains."

The intent of the survey is to identify how U.S. companies are sourcing mature-node semiconductors, also known as legacy chips. This analysis will inform U.S. policy to bolster the semiconductor supply chain, promote a level playing field for legacy chip production, and reduce national security risks posed by the People's Republic of China (PRC).

The assessment was requested by the Secretary of Commerce in response to findings in a Congressionally mandated report released in December 2023 that assessed the capabilities of the U.S. microelectronics industrial base to support U.S. national defense. The findings of that report, titled "Assessments of the Status of the Microelectronics Industrial Base in the United States," are available online at: https://www.bis.doc.gov/index.php/other-areas/office-oftechnology-evaluation-ote/industrial-base-assessments

The survey will be performed under Section 705 of the Defense Production Act of 1950 to evaluate the extent of, and visibility into, the use of mature-node chips manufactured by PRC-based companies in supply chains of critical U.S. industries like telecommunications, automotive, medical device, and the defense industrial base.

87. Does the Department of Commerce believe tariff authorities play a role in preventing the PRC from dominating the U.S. market for legacy semiconductors?

The Department will continue working with our executive branch colleagues and will not hesitate to appropriately use its tools to address national security threats posed by the PRC.

88. Has the Department of Commerce approved export control licenses to provide the PRC with the semiconductor manufacturing equipment they need to build out their legacy semiconductor capacity?

The Department and its interagency partners at State, Defense, and Energy review and approve licenses for the export of items subject to Commerce's jurisdiction under the process outlined in Executive Order 12891 and pursuant to the licensing policies identified in the EAR.

Any exports of certain tools subject to U.S. jurisdiction would be subject to such a review process.

In addition, the updates issued by BIS on October 17, 2023, that took effect on November 17, 2023, expanded the list of semiconductor manufacturing equipment subject to U.S. controls beyond the list outlined in the October 7, 2022, rule issued by BIS.

Further, on January 18, 2024, BIS released an industrial base survey under its Defense Production Act authorities into mature node semiconductors. Secretary Raimondo stated, "Legacy chips are essential to supporting critical U.S. industries, like telecommunications, automotive and the defense industrial base. Addressing non-market actions by foreign governments that threaten the U.S. legacy chip supply chain is a matter of national security. Over the last few years, we've seen potential signs of concerning practices from the PRC to expand their firms' legacy chip production and

make it harder for U.S. companies to compete. To get ahead of these concerns, the Department of Commerce is taking proactive measures to assess the U.S. semiconductor supply chain by collecting data from U.S. companies on the sourcing of their legacy chips. Government alone cannot create and sustain a robust supply chain—we need industry at the table. This survey will empower the Department with the data we need to inform our next steps in building strong, diverse, and resilient semiconductor supply chains."

The intent of the survey is to identify how U.S. companies are sourcing mature-node semiconductors, also known as legacy chips. This analysis will inform U.S. policy to bolster the semiconductor supply chain, promote a level playing field for legacy chip production, and reduce national security risks posed by the People's Republic of China (PRC).

The assessment was requested by the Secretary of Commerce in response to findings in a Congressionally mandated report released in December 2023 that assessed the capabilities of the U.S. microelectronics industrial base to support U.S. national defense. The findings of that report, titled "Assessments of the Status of the Microelectronics Industrial Base in the United States," are available online at: https://www.bis.doc.gov/index.php/other-areas/office-oftechnology-evaluation-ote/industrial-base-assessments

The survey will be performed under Section 705 of the Defense Production Act of 1950 to evaluate the extent of, and visibility into, the use of mature-node chips manufactured by PRC-based companies in supply chains of critical U.S. industries like telecommunications, automotive, medical device, and the defense industrial base.

More information on the survey is available online at: https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3437-2024-01-18-bis-press-release-legacy-chip-survey-final/file.

89. Does the Department of Commerce believe PRC semiconductor firm CXMT has ties to the PLA?

90. Why does the Department of Commerce believe PRC semiconductor firm CXMT should not be on the Entity List — as evidenced by the fact that it is not listed?

Answer to questions 89 and 90. The Department and its interagency colleagues remain vigilant in addressing concerns related to firms that may be supporting the PRC's military modernization and will not hesitate to take action as appropriate to protect U.S. national security and foreign policy interests, as evidenced by the powerful PRC-wide export controls on advanced semiconductors and semiconductor manufacturing equipment put in place in October 2022 and updated and expanded in October 2023, and through vigorous use of the Entity List. Under the Biden Administration over 1,100 entities (over 40 percent of all entities) have been added to the Entity List, including over 300 in the PRC. BIS and our interagency partners, particularly at State, Defense, and Energy, but in concert with other agencies as appropriate and with support from the intelligence community, assess all-source information when developing, implementing, and enforcing export controls.

91. If the Department of Commerce knew that U.S. technology was going to a PRC firm that was assisting the PLA or any other PRC or CCP intelligence or security agency, would it deny the license?

License applications are reviewed for national security and foreign policy concerns by the Departments of Commerce, State, Defense, and Energy with additional support and insight from the intelligence community. The interagency carefully reviews license applications to the PRC for risk of diversion to the PLA or CCP intelligence or security agencies and makes determinations on those licenses based on U.S. national security and foreign policy considerations.

92. Does the Department of Commerce believe there is such a thing as a truly "private" company in the PRC?

Over the past several years, the PRC's leaders have made clear that they do not plan to pursue political and economic reform and are instead pursuing an alternative vision of their country's future. They are committed to increasing the role of the state in society and the economy, constraining the free flow of information, and decoupling economically in a number of areas, including many technology sectors of the future. They have firewalled their data economy from the rest of the world. And they are accelerating their efforts to fuse their economic and technology policies with their military ambitions. The legal system and concepts related to the regulation of various enterprises in the PRC are very different from how similar enterprises are understood and regulated under U.S. law.

93. What is the Commerce Department's role in Integrated Deterrence, especially when it comes to near-term deterrence of an invasion of Taiwan?

The Commerce Department employs an "offense/defense" strategy that seeks to promote the strength of the U.S. economy and innovation ecosystem through initiatives such as the CHIPS and Science Act, Bipartisan Infrastructure Law, and Inflation Reduction Act and other initiatives, and through "defensive" activities such as export controls that seek to prevent foreign adversaries including the PRC from obtaining U.S.-origin items that they seek to employ for military modernization and other activities that present national security or foreign policy concerns.

A key component of these efforts is international engagement and working to bring U.S. partners and allies on board with initiatives such as export controls. The Biden Administration has been successful in marshalling such a coalition to respond to Russia's invasion of Ukraine, and also worked to build partnerships and coordination through the U.S.-EU Technology and Trade Council, Indo-Pacific Economic Framework for Prosperity (IPEF), and other initiatives.

These efforts contribute to the Administration's overall integrated deterrence efforts, alongside other initiatives led by other departments such as Defense and State. Export controls are an important tool in the U.S. government toolbox, but they are not the only tool. Any response to a kinetic action by the PRC against Taiwan would be a

whole of government effort and BIS would take appropriate action, in coordination with the interagency and in consultation with allies and partners.

94. What specific actions is Commerce taking to coordinate export control packages or other responses with allies ahead of time in order to hopefully deter a crisis involving the PRC?

As outlined in the Export Control Reform Act of 2018 (ECRA), export controls that are imposed on a multilateral basis are generally more effective and durable than export controls imposed unilaterally. The Department continues to work through existing export control regimes (Wassenaar Arrangement, Australia Group, Missile Technology Control Regime, and Nuclear Suppliers Group) as well as through others such as the U.S.-EU Trade and Technology Council (TTC) and Indo-Pacific Economic Framework (IPEF) to ensure that international allies and partners understand the threat context as we see it, and encourage them to adopt similar controls. Commerce also recognizes that there are circumstances where existing structures may not be sufficient, such as in the case of Russia's invasion of Ukraine. In response, the United States has marshalled a Global Export Control Coalition of 38 international partners that has worked to deny the Russian industrial base the items it seeks to sustain its military efforts. In addition, certain key supplier governments imposed comparable controls on semiconductor manufacturing equipment after the United States took action in October 2022. Such coordination and activities demonstrate the power of partnerships and serve as a potential template that can be employed in future exigencies if appropriate.

95. What specific actions can the Commerce commit to taking to strengthen near-term Integrated Deterrence when it comes to Taiwan?

The Department's ongoing international engagement efforts, as identified in response to 93 and 94, contribute to overall regional and global security efforts and the Department will continue working to further them to strengthen the global security environment in pursuit of a peaceful, secure, rules-based international order.

Representative Andy Barr – District KY-08

96. DOD and Commerce each maintain lists of entities that they view in various degrees as risks to national security.

a. The DOD 1260H list is a list of Chinese military companies" operating directly or indirectly in the United States.

b. Commerce maintains several lists—the Entity List, Military End User List, Denied Persons List.

A/S Kendler—When you are looking at entities to add to commerce lists, is your agency looking at the DOD 1260H list? Can you tell this committee how many 1260H companies are on Commerce lists?

The Department of Defense is a member of the End-User Review Committee which, under the Export Administration Regulations (EAR), makes all determinations for additions, modifications, or removals to the Entity List. Additions to the Entity List require a majority vote of the End-User Review Committee (ERC), which is chaired by Commerce, with representation from the Departments of State, Defense, Energy, and where appropriate, the Treasury. The ERC determines whether the entity has been involved in, is involved in, or poses a significant risk of being or becoming involved in activities that are contrary to the national security or foreign policy interests of the United States. Any member of the ERC may make nominations for the addition of entities to the Entity List and Military End User (MEU) List.

As of February 2, 2024, the DOD's 1260H list contains 46 entities and their subsidiaries and affiliates. The Entity List contains over 2,300. A number of entities on the 1260H list are also on lists administered by BIS either in full, or certain subsidiaries and affiliates that have been found by the ERC to be acting contrary to U.S. national security or foreign policy interests.

The Entity List maintained by BIS imposes license requirements on the export, reexport, or transfer (in-country) of items subject to the EAR to or involving as parties to the transaction entities identified on the Entity List, all of which must be foreign entities, and all of which must be determined to have been, are currently, or are at significant risk of becoming, involved in activities contrary to U.S. national security and foreign policy concerns. The 1260H list is developed based on different criteria.

Different agencies have different authorities that can be applied in a variety of circumstances to address particular conduct, and each of these authorities have their own distinct criteria for the designation of specific entities. BIS engages with other agencies as appropriate to coordinate on measures to protect U.S. national security and foreign policy interests. As a consequence, different lists may have different firms, individuals, or other entities, but depending upon the specific facts and circumstances, there may be overlap across one or more different lists.

For example, in the Russia sanctions context, many entities have been designated by Treasury pursuant to Executive Order 14024 (Blocking Property With Respect To Specified Harmful Foreign Activities of the Government of the Russian Federation, April 15, 2021) and were also added to the BIS Entity List.

In addition, in certain instances, the EAR apply restrictions on exports and reexports to persons designated pursuant to Executive Orders administered by the Department of the Treasury as well as pursuant to select sanctions statutes. In these instances, when a person is identified and sanctioned pursuant to the applicable authority (e.g., an Executive Order or statute), BIS imposes license requirements on transactions involving items subject to the EAR that are destined to the sanctioned person or to which they are a party.

97. A/S Kendler—Would listing on the 1260H list mean an automatic denial of a license to a company seeking to do business with a 1260H company?

Please see response to question 96. Export license applications are reviewed by the interagency (Commerce, Defense, State, and Energy).

Representative John Moolenaar – District MI-02

98. Assistant Secretary Kendler, in your written testimony you said, "The CCP under President Xi Jinping has set a goal to overtake the United States and its allies by dominating certain advanced technology sectors." You also wrote that the "CCP uses a military civil-fusion strategy to deliberately blur lines between commercial sectors and military programs, "and that the [CCP] government demands "information and assistance from companies that have little choice but to agree."

a. Given that you seem to understand Xi Jinping's goals, do you think the United States should allow companies that pledge allegiance to the CCP and President Xi to build factories in our country?

Pursuant to the authorities provided by Congress, the Committee on Foreign Investment in the United States (CFIUS), which is chaired by the Department of the Treasury, reviews any transaction that could result in foreign control of a U.S. business; certain non-controlling, non-passive transactions by foreign persons in certain U.S. businesses involved in critical technology, critical infrastructure, and sensitive personal data; and transactions by foreign persons involving real estate in proximity to sensitive government facilities or properties

and certain air and maritime ports. While the Commerce Department is a member of CFIUS, this inquiry would be more appropriately directed to Treasury.

99. Representative Darin LaHood – District IL-16 I'm concerned about recent reports that the DOJ and FTC have removed technology standards in the Indo-Pacific Economic Framework that are designed to protect U.S. companies from Chinese-style censorship and discrimination in the region. We are seeing China successfully push its regulatory model in countries like Indonesia and Vietnam that are adopting data localization and censorship requirements intended to make it easier for Chinese tech firms to grow and prosper. Why has the Administration abandoned efforts to counter PRC's technological influence in the Indo-Pacific region? Do you believe that it is a good strategy to remove or water down key digital rules in the Indo-Pacific Economic Framework that constrain discriminatory digital regulations and Chinese-style data flow and censorship barriers?

Questions related to negotiation of digital trade provisions in trade provisions would be best directed to the Office of the U.S. Trade Representative, which is leading negotiations for the United States on Pillar I (Trade) of the Indo-Pacific Economic Framework for Prosperity (IPEF).

Representative Seth Moulton – District MA-06

100. How do China's economic challenges create opportunities or leverage for the United States?

The current environment provides a further opportunity to press our PRC counterparts to make policy changes that address U.S. concerns and would support the Chinese economy, while being clear-eyed about the many challenges to our existing relationship.

As Secretary Raimondo articulated on her August trip to China, on matters of national security, there is no room to compromise or negotiate. However, the vast majority of our trade and investment relationship does not involve national security concerns and in this regard, and we are not seeking the decoupling of our economy from that of China's. The Department is committed to promoting trade and investment in those areas that do not undermine our interests or values, while using all the tools at our disposal to protect our companies and counter unfair economic practices.

President Biden has been crystal clear repeatedly on this point; we seek healthy competition with the PRC. A growing economy in China that plays by the rules is in both of our interests. That said, we have to make sure there is a level playing field because no one can outcompete the United States if we are playing by the same rules.

Please complete a separate sheet for each witness that you wish to submit additional questions to. Fill in your Representative name, district, and the witness name the questions are to be sent to. Return completed form(s) to Austen.adcock@mail.house.gov by 7:00pm on July 20th.