January 17, 2024

The Honorable Alan F. Estevez
Undersecretary of Commerce for Industry and Security
U.S. Department of Commerce
1401 Constitution Avenue N.W.
Washington, DC 20002

Regulations.gov docket no. BIS-2022-0025
RIN 0694-A194

Dear Under Secretary Estevez,

The National Foreign Trade Council ("NFTC") notes the Bureau of Industry and Security's ("BIS") recent publication of two Interim Final Rules ("IFR"), issued October 17, 2023, on Additional Export Controls on Advanced Computing Items, Supercomputer, and Semiconductor End-Use ("AC/S") and Semiconductor Manufacturing Equipment and Related Equipment to China ("SME"), both of which seek input from interested stakeholders. The NFTC appreciates this opportunity to provide comments on the AC/S IFR.

Remote access and cloud computing

NFTC understands that BIS is considering imposing additional restrictions on "remote access" to advanced AI chips. Historically, BIS has taken the position that "cloud services" do not involve an export and therefore would not be subject to export control restrictions. NFTC urges BIS to remain consistent with longstanding precedent regarding grid and cloud computing services.

In an Advisory Opinion issued January 13, 2009, BIS held that the "The service of providing computational capacity would not be subject to the EAR as the service provider is not shipping or transmitting any commodity, software or technology to the user." This was affirmed in an Advisory Opinion dated January 11, 2011, stating that "…. The service of providing computational capacity through grid or cloud computing is not subject to the EAR," and "Because the service provider is not an "exporter" [company] would not be making a deemed export…" On November 13, 2014, BIS issued an Advisory Opinion regarding cloud-based storefronts stating that "… there is no export of software in the cloud-based storefront fact pattern".

NFTC recognizes that certain entities pose a heightened national security threat due to the risk of using advanced AI chips for weapons development or other military purposes and supports

the continued use of additional controls through designation on the Entity List and Military Intelligence End-user List. We discourage the implementation of country-wide controls as overly broad and unilateral controls that risk further accelerating China's indigenous development of advanced AI chips and driving Chinese users and other multinational companies to Chinese Infrastructure-as-a-Service (IaaS) providers to the detriment of American companies.

IaaS

We recognize that the immense geopolitical significance of Artificial Intelligence (AI) demands a thoughtful approach for limiting access to high-performing Artificial Intelligence (AI) chips and related equipment to entities that present national security concerns. We support BIS's objective to protect U.S. national security and appreciate that BIS is seeking input on the possibility of expanding AI-related export controls to IaaS due to the complexities of this topic. We welcome the opportunity to comment on these important issues and hope these comments will aid the agency in achieving its objective.

IaaS is the backbone of the digital economy and the world's technological security infrastructure, and an engine of economic growth for the United States, supporting U.S. jobs and contributing to the U.S. export base. U.S. IaaS providers are global leaders in the industry, providing the most secure, reliable, and innovative products and services to hundreds of millions of customers around the world. U.S. leadership on IaaS is critical to U.S. national security, ensuring that the United States remains at the forefront of the development of technologies that are central to the world's security infrastructure and global economic growth.

Export controls on IaaS, unless carefully and narrowly drawn and truly essential to national security, would hurt U.S. IaaS providers and U.S. competitiveness globally and threaten U.S. national security. Overly broad controls risk reducing U.S. IaaS providers' sales to global customers, stifling their innovation and technological advancement, and impeding the adoption of their technologies worldwide. Importantly, it would also cause companies all around the world to build their technology off of Chinese or other foreign IaaS providers, which at best causes a significant US economic impact and at worst, triggers also a material security vulnerability for the United States.

These grave consequences would come at a critical time for the IaaS industry, as customers around the world are seeking to take advantage of groundbreaking AI/ML technologies powered by IaaS. Although the United States is currently a global leader in IaaS, other countries are advancing in the industry, particularly China, which has the largest IaaS providers outside of the United States (e.g., Huawei, Alicloud, Tencent). Many European countries are also seeking to build their own IaaS champions and are leveraging extraterritoriality and continuity of service concerns around U.S. laws—including concerns about loss of access to U.S. technologies due to sanctions—to advance a digital sovereignty agenda and regulatory actions (e.g., the European Cybersecurity Certification Scheme for Cloud Services) that discriminate against and seek to exclude U.S. companies. Overly broad and discretionary export controls would reinforce fears about dependence on U.S. technology companies and put U.S. IaaS providers at a competitive disadvantage. Such efforts could drive customers to foreign IaaS providers – ultimately furthering the growth of foreign competitors, including in China, and costing high-paying U.S. jobs.

Any export controls should apply equally to U.S. and non-U.S. IaaS providers. Consistent with longstanding BIS policy, the provision of IaaS is not an export therefore controls should apply to

the customer(s) of the IaaS provider. However, to the extent BIS now deems it necessary to impose restrictions on IaaS providers, they should apply equally to U.S. and non-US providers. To ensure equal applicability, BIS should pursue multilateral cooperation on controls, rather than imposing unilateral controls that apply only to U.S. IaaS providers. Such unilateral controls would disadvantage U.S. industry in favor of primarily Chinese providers, which is inconsistent with policy objectives and undermines U.S. national security goals by driving customers to non-U.S. IaaS providers to develop models without constraints. U.S. IaaS providers have strong responsible use guidance and terms of service in place with customers. The U.S. government should encourage the development of AI on IaaS providers, which have strong responsible use guidance and terms of service in place with customers and have committed to voluntary principles for responsible AI development. Foreign competitors including Chinese companies may not have signed onto the same responsible AI policies, further undermining U.S. national security.

Export controls must not inadvertently or disproportionately impede U.S. competitiveness, economic growth and technological leadership. Controls should be narrowly and specifically tailored to address essential and clearly defined U.S. national security interests. Controls should be targeted to compute capacity derived from advanced AI chips already subject to export controls. Overly broad controls that restrict U.S. IaaS providers from full participation in the global industry undermine U.S. technological leadership. In addition to accelerating the global adoption of non-U.S. IaaS products and services, this would undercut U.S. leadership on the development and adoption of critical industry standards. Particularly as the adoption of AI/ML and other sensitive technologies accelerates, the U.S. must remain on the front lines of the global technology economy and able to shape the development and adoption of these technologies including safety and security standards.

The AC/S IFR posed questions for commenters. Please see Attachment, which contains our responses to several of these questions. NFTC appreciates the opportunity to provide this additional input.

General Comments

NFTC appreciates the public briefing held by Assistant Secretary Thea Rozman Kendler on November 6, 2023 as well as the FAQs published on December 29, 2023. However, we note that delays in implementing License Exception NAC (Notified Advanced Computing) created initial confusion about this new License Exception. For example, NAC appears to be designed for semiconductor companies and not downstream users of chips including AI chips. In many cases downstream users including OEMs who actually engage in exports will not have the information required by NAC.

Other ambiguities in both the AC/S and SME rules require human oversight to ensure compliance, thus increasing burden and cost. Additionally, some extraterritorial requirements are prohibited by foreign jurisdictions. This appears to conflict with the Export Control Reform Act (ECRA) section 4812(b)(3), which explicitly requires the President, when exercising end use authorities, to “seek to secure the cooperation of other governments and multilateral organizations to impose control systems that are consistent, to the extent possible, with the controls imposed under subsection (a).” Therefore, BIS should describe, to the extent permissible and consistent with the objective of developing plurilateral end use controls, what steps it has taken to level the regulatory playing field for US industry with respect to the end use

controls in section 744.6 and 744.23; and commit to working quickly and aggressively with the allies to convince them to adopt comparable end use controls. Multilateral efforts are necessary to ensure the effectiveness of EAR end-use controls and satisfy ECRA requirements.

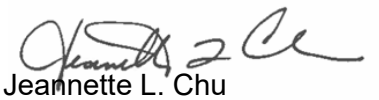
Members have also expressed concerns about future controls. While we understand and support the need to maintain technological leadership, constantly changing controls can cause significant disruption particularly to supply chains where resource commitments are made far in advance. Also concerning is the growing complexity of determining incremental license requirements. This impacts business continuity, creates potential delays to shipments, and impacts technology roadmaps involving geo-expansion plans. Such delays can be very costly and ultimately negatively affect the competitiveness of U.S. businesses.

About NFTC

The NFTC, organized in 1914, is an association of U.S. business enterprises engaged in all aspects of international trade and investment. Our membership covers the full spectrum of industrial, commercial, financial, and service activities. Our goal is to always protect national security and economic security interests and strengthen U.S. industries. Robust trade relationships are central to economic and national security. Through the Alliance for National Security and Competitiveness, NFTC's National Security Policy Initiative brings the voice of business to policy makers on global security issues affecting international trade.

Thank you for your consideration of our comments and for your continued engagement with industry. We welcome the opportunity to discuss this important matter and to answer any questions that you may have. I can be reached at (202) 887-0278 or via email to jchu@nftc.org.

Sincerely,



Jeannette L. Chu
Vice President for National Security Policy
Executive Director, Alliance for National
Security and Competitiveness

ATTACHMENT to comment letter on AC/S IFR
Regulations.gov docket no. BIS-2022-0025
RIN 0694-A194
January 17, 2024

BIS Question 1: Addressing access to "development" at an IaaS provider by customers developing large dual-use AI foundation models with potential capabilities of concern

NFTC understands the U.S. Government's interest in preventing diversion of AI chips, but the same risk of diversion is not present when a customer accesses the compute capacity of an AI chip via an IaaS provider, as they do not obtain physical possession of the chips themselves. However, should BIS be determined to proceed in this area, we strongly encourage that BIS apply a targeted approach to mitigate risks related to IaaS, while minimizing the impact on U.S. IaaS providers and the U.S. position as a global technology leader. Specifically, any IaaS-related export controls should be narrowly tailored, including by applying:
1. only to compute power from AI chips that are already subject to export controls (i.e., any forthcoming controls should be consistent with October 25 IFR controls);
2. only to compute capacity at the threshold necessary to develop large, highly capable foundation models;
3. alignment and interoperability with the Executive Order on Safe, Secure and Trustworthy Artificial Intelligence ("AI EO") and its forthcoming implementing regulations;
4. only to specific entities that pose national security risks;
5. any applicable export license or notification requirement should apply only to the IaaS user and not the provider; and
6. to U.S. and non-U.S. companies alike.

BIS Question 4: Applicability of Deemed Exports and Deemed Reexports

NFTC very much appreciates that deemed exports were exempted from this IFR. If they had not been exempted, industry would have faced significant compliance challenges. For example, some of the best AI and datacenter scientists and engineers, whose work requires access to advanced AI technologies, are foreign nationals. Having to obtain a license for such foreign nationals would drastically slow down innovation; moreover, because there is a presumption of denial for licenses to China, a meaningful proportion of this workforce would be unable to contribute to further innovation. Rather than attracting foreign-born talent to the U.S. this would cause more engineers to remain overseas and contribute to AI development abroad, ultimately having a negative impact on U.S. national security.

Application of 15 C.F.R. § 742.6(a)(6)(iv) to deemed exports and deemed reexports would significantly reduce U.S. technology companies' ability to recruit and develop both U.S. and non-U.S. talent. In many instances, the internal security and trade-secret protection procedures of companies working with the restricted semiconductor technology may be as, if not more,

effective than deemed export licensing to protect against the risk of diversion. Companies invest significant resources in the development of technologies, and it is in the companies' economic interest to ensure proprietary technologies remain protected from third parties.

Today, U.S. companies are able to develop many of the restricted semiconductor technology because of significant recruiting efforts to attract the world's top talent—both U.S. and non-U.S.—within particular technological disciplines. Top U.S. scientists and engineers want to collaborate with the best scientists and engineers from around the world, regardless of nationality or location. Placing restrictions on their ability to do so would discourage top U.S. talent from accepting positions in the United States or with U.S.-based companies, sending that talent offshore where these restrictions do not apply to foreign companies. There is already an existing shortage of talent that can develop cutting edge semiconductors. Deemed export or deemed reexport restrictions would further exacerbate the issue further, increase the cost of hiring talent, and delay projects that are already underway. Deemed export and deemed reexport restrictions damage companies' ability to compete in the open global marketplace for top talent, undermines U.S. leadership in the semiconductor technology, and negatively impacts the U.S. economy.

.

We strongly discourage BIS from imposing new deemed export or deemed reexport controls. We encourage BIS to maintain the current carve out under 15 C.F.R. § 742.6(a)(6)(iv), and to consider whether companies' own security and intellectual property-focused protections would supplant or exceed any benefits that could be gained through deemed export and deemed reexport requirements.

BIS Question 5: Designed or Marketed for Data Centers

In order to use License Exception NAC (Notified Advanced Computing) Ifor ECCN 3A090.a, an entity must first determine whether the chip is "designed or marketed for use in datacenters." For companies reselling chips made by other companies, it is not possible or practical to know whether a chip is "designed or marketed for use in datacenters" as these companies only market the chips. To address this concern, we suggest that BIS modify the following 3A090 subparagraph by adding the language ***in bold*** to explicitly assign an ECCN for items that are designed or marketed for use in datacenters. This approach will allow manufacturers to use the ECCN to communicate the correct level of control and identify the appropriate compliance requirements within automated systems. For example, if a manufacturer used proposed ECCNs 3A090.a.1.a and 3A090.a.1.b and communicated those to a reseller, the reseller would be able to easily determine if the item requires a license or is NAC eligible, respectively.

Proposed revisions:

> a. Integrated circuits having one or more digital processing units having either of the following:
>
> a.1. a 'total processing performance' of 4800 or more and ***meeting the following****:*

a.1.a designed or marketed for use in datacenters

a.1.b designed or marketed for use for any application other than those identified in a.1.a

or:

a.2. a 'total processing performance' of 1600 or more and a 'performance density' of 5.92 or more.