Alliance for Network Security on Implementation of Additional Export Controls: Certain Advanced Computing Items; Supercomputer and Semiconductor End Use; Updates and Corrections

Comment uploaded to: https://www.regulations.gov/commenton/BIS-2022-0025-0052

Public Comment
Due Date: January 17, 2024

Bureau of Industry and Security
US Department of Commerce
1401 Constitution Avenue NW
Washington, DC 20230

Re: Additional Export Controls – BIS-2022-0025 – RIN 0694–AI94 – 88 FR 73458 (October 25, 2023)

Dear Sir / Madam:

Thank you for this opportunity to comment on the Interim Final Rule published on October 25, 2023 (88 FR 73458), implementing controls on advanced computing integrated circuits (ICs), computer commodities that contain such ICs, and certain semiconductor manufacturing items, and to make other changes to implement appropriate related controls, including on certain "US person" activities, under the Export Administration Regulations (EAR, 15 CFR 730 *et seq.*).

This comment is submitted by the Alliance for Network Security (ANS) whose members consist of leading Information Technology companies that make widespread use of encryption, among other technologies. ANS hereby responds to Requests for Comment No. 1, 4, 5, 6, and 7, as well as provides additional information for consideration by the Bureau of Industry and Security (BIS).

Request for Comment No. 1: Development at an Infrastructure as a Service (IaaS) Provider

Before imposing any new controls related to IaaS, BIS should take into account the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (EO 14110, October 30, 2023). This EO establishes new requirements around reporting and identity verification of foreign purchasers of high capability US IaaS products and, as such, appears to address the national security risks BIS is seeking to target. To avoid duplication of effort and establishment of multiple, overlapping regulations, BIS should focus on the EO and refine and implement its regulations to address national security concerns related to the use of IaaS products for the development of large dual-use AI foundation models. It will be important, in particular, to observe and assess the implementation and operation of the EO's regulations, both in terms of their effectiveness, and any difficulties in implementation, before imposing new export control requirements with respect to the same products. That said, to the extent that there is contemplation of additional export control regulations, we offer the following considerations.

IaaS providers ordinarily do not and should not monitor their customers.

Any additional regulations in this area should take into account the significant challenges that IaaS providers would face if asked to identify whether a customer has developed a "dual-use AI foundation model." The EO's definition of "dual-use foundation model" includes the criteria that the AI model exhibit high levels of performance at tasks that "pose a serious risk to security, national economic security, national public health or safety." IaaS providers generally do not have visibility into their customers' workloads due to security, privacy, and related requirements, and usually would not have access to a customer's AI model to determine whether it exhibits such characteristics. IaaS customers typically consider information about the amounts or types of training data being used, the number of parameters, and the methods of training AI models to be sensitive, proprietary information, and are unlikely to be willing to share such information with IaaS providers.

Many factors that have been suggested as a basis for regulating models cannot be determined before training is completed.

Any regulations should also consider IaaS providers' need for controls based on objective criteria that are clear at the outset of providing services to a customer and avoid relying on characteristics that cannot be determined until after a model has been trained. IaaS providers—indeed, even the customers themselves—cannot be certain what levels of performance a model will exhibit at particular tasks until after training is complete. Also, IaaS providers cannot know in advance of providing services how many operations will be used in training the customer's model. The number of chips used by the customer in training has some impact on this, but key determinative factors like training time and training efficiency are not visible to IaaS providers until after training.

Preserving the EAR's existing approach to IaaS remains essential.

BIS should not abandon the 2009[1], 2011[2], and 2014[3] advisory opinions regarding cloud computing. These advisory opinions are well-reasoned and reflect the distinct differences between interacting with hardware and software via the cloud in contrast to owning or having physical control over the hardware or software. They also recognize the practical realities of the provision of computational capacity and correctly establish that provision of computational capacity is not an export and an IaaS provider is not the exporter when providing computational capacity. These advisory opinions have enabled US leadership in IaaS and SaaS business models, supporting US economic and national security interests by ensuring the United States

[1] Application of EAR to Grid and Cloud Computing Services, https://www.bis.doc.gov/index.php/documents/advisory-opinions/527-application-of-ear-to-grid-and-cloud-computing-services/file.
[2] Cloud Computing and Deemed Exports, Application of EAR to Grid and Cloud Computing Services, https://www.bis.doc.gov/index.php/documents/advisory-opinions/527-application-of-ear-to-grid-and-cloud-computing-services/file.
[3] Advisory Opinion on Cloud-based Storefronts, https://www.bis.doc.gov/index.php/component/docman/?task=doc_download&gid=1098&Itemid=182.

remains at the forefront of the development of technologies that are central to the world's security infrastructure and global economic growth. Abandoning these advisory opinions and imposing IaaS-related export controls risks undermining the US IaaS industry and US competitiveness globally and threatening US national security.

Expansive IaaS-related controls would drive customers to foreign competitors and undermine US national security.

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). European countries and other foreign customers are already concerned that US technology providers are unreliable due to continuity of service concerns around the extraterritorial application of US laws, and the expanded scope of the October 25 controls to 40+ countries and all Chinese companies globally risks reinforcing concerns that American companies are not reliable global suppliers of technology. Imposing similarly broad controls related to IaaS would bolster this narrative and place US IaaS providers at a competitive disadvantage. If potential customers face hurdles or potential restrictions in accessing US technology, they will simply look elsewhere, including to Chinese or other foreign providers, rather than risk losing access to critical IaaS technologies. This result will undercut the US IaaS industry and cost American jobs, while also threatening US national security by shifting the development of AI models and technology builds to foreign providers that may not have the same interests in privacy, security, and responsible AI as US providers.

Some sources have suggested that imposing export controls on IaaS is required in order to mirror the expansion of controls on 3A090 chips and thereby close a "loophole" created by customers accessing the chips via cloud versus through physical possession. There is no such loophole.

Training large dual-use AI foundation models currently requires thousands of chips connected with highly performant networking and supported by other specialized infrastructure, like cooling. If someone gains physical possession of a 3A090 chip, they can physically connect that chip with others to create a cluster for use in training a dual-use AI foundation model. By contrast, an IaaS customer would not have that capability. This is because the ability to utilize small numbers of 3A090 chips made available by IaaS providers does not provide customers with the ability to independently aggregate those chips into a cluster capable of training a large dual-use AI foundation model without that aggregation being directly enabled by the IaaS provider.

It is important to understand the complexity and expertise involved in setting up and managing the infrastructure required to train large dual-use AI foundation models. It is not simply a matter of possessing AI chips; it also involves network infrastructure, cooling systems, and software for managing and coordinating the computation. Additionally, while IaaS providers do offer access to AI chips, customers typically cannot use them to build large-scale clusters without being directly enabled by the IaaS provider.

Moreover, as discussed above, a foreign IaaS customer using a large 3A090 run will already be subject to reporting via the mechanisms established in Section 4.2(c) of the EO. Those mechanisms should be developed, and their efficacy assessed, before any further regulatory action is undertaken.

In Summary

BIS's advisory opinions have not only driven the US economy, created many jobs, and enabled US cloud computing providers to be the global leaders in this space; they also have benefitted US national security by having companies headquartered in countries deemed to be foreign adversaries choose US platforms rather than others with different values and less oversight. Overly restrictive requirements risk driving IaaS customers to choose non-US providers, which is not in the United States' economic or national security interests. BIS's historical export controls tools, such as licensing on particular products, should be avoided for IaaS. BIS should first rely on the AI EO reporting requirements that will provide the US government with important information that can be used to assess the scope of the risks and determine the appropriate policy approach.

Request for Comment No. 4: Deemed Exports and Deemed Reexports

The carveout for deemed exports on technology for 3A090 (and associated 4A090 and .z) items has had a significant positive impact on US leadership in developing these chips. The EO identified the importance of attracting non-US talent to work in AI fields in the United States, but deemed export licensing requirements would directly undermine efforts to ensure that the most talented chip developers can contribute to US companies' efforts to ensure that US companies remain the leading chip developers in the world. Otherwise, such talent is likely to go to other countries, including foreign competitors and even adversaries.

The practicalities of recruiting talent and obtaining deemed export licenses create severe challenges for employees and employers. Other US government regulations regarding employment discrimination generally do not allow for consideration of whether the employee would need a deemed export license when making hiring decisions. Given the lengthy processing times for the US government to review deemed export license applications and, in the case of approved licenses, determine the conditions that should attach to the license, employers must decide to either push back start dates or allow the employee to start work without being able to perform their intended responsibilities. Individuals who face the uncertainty of whether or when they will be able to perform the work they were hired to do may choose to forgo working on export controlled projects that contribute to US leadership in important fields. The need to obtain and renew deemed export licenses also creates uncertainty for medium- and long-term planning for projects subject to heightened controls. ECCN 3E002 already applies to technology used in many 3A090 chips, which would make deemed export license requirements on 3E001 technology for 3A090 chips redundant in many cases.

In general, the deemed export licensing experience has led to negative and counterintuitive outcomes. The frequent practice of imposing overly restrictive license conditions has led to situations in which licenses are granted but in practice prevent the applicants from performing their intended work. In several cases, deemed export licenses for non-US nationals with world-class expertise have included conditions so restrictive as to make the licenses practically useless. Shortly thereafter, the same individuals were granted US person status by relevant agencies and were thus no longer subject to deemed export licensing requirements. Such a dynamic does not serve either US national security objectives or US companies' business goals, and it seems to suggest that government agencies making decisions about deemed export licenses are applying stricter criteria than the agencies making decisions to extend the broader, more significant benefits of becoming a US person.

In Summary

The deemed export requirements on technology for AI chips and associated items could potentially create a significant barrier to innovation and progress in the United States. These requirements could deter talented international chip developers from contributing to US-based companies, which could have several negative impacts:

1. **Loss of Competitive Edge**: The United States is currently a global leader in chip development. However, if we lose access to international talent, our competitive edge could be at risk. Other countries, including our competitors and adversaries, could benefit from the expertise that would have otherwise contributed to US advancements.
2. **Stifling Innovation**: Diversity is a key driver of innovation. Having a diverse team of developers from different backgrounds and cultures can lead to more creative and effective solutions. By limiting who can contribute to US companies on AI chip development, we could be stifling potential innovation.
3. **Economic Impact**: The chip development industry is a significant contributor to the US economy. If US companies lose their leading position in this field, it could have serious economic consequences.
4. **National Security**: Advanced chip technology is crucial for many aspects of national security. If the United States falls behind in this area, it could potentially compromise our national security.

Therefore, it is critical to maintain the deemed export carveouts to ensure the United States continues to attract top talent, maintain its competitive edge, foster innovation, support the economy, and safeguard national security.

Request for Comment No. 5: Control Parameters Under 3A090 and Note 2

Control List Text for ECCN 3A090.a.1

In order to use License Exception NAC for 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 more burdensome and impractical to know whether a chip is "designed or marketed for use in datacenters".

To address this concern, we suggest BIS modify the following ECCN 3A090 subparagraph 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 to the control list text to ECCN 3A090.a.1 in red and underlined:

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, or

a.1.b designed or marketed for use for only applications other than datacenters,

or,

License Exception NAC Eligibility for ECCN 3A090.a.2

Eligible items for License Exception NAC include ECCN 3A090.b items (if designed or marketed for datacenters) and ECCN 3A090.a items (if not designed or marketed for datacenters). ECCN 3A090.a.2 items, which under Note 2 are by definition designed or marketed for datacenters, are currently not eligible for License Exception NAC. We request that License Exception NAC be amended to allow for use in exporting 3A090.a.2 items.

Per the October 17, 2023 Interim Final Rule, BIS is providing License Exception NAC for the less powerful advanced ICs. Note 2 to ECCN 3A090 demonstrates the US government's determination that advanced ICs with a TPP less than 4800 should be considered as a category of less powerful advanced ICs.

Indeed, Note 2 specifies that any item with a TPP performance below 4800 that is not designed or marketed for datacenters is not even controlled by ECCN 3A090.

Extending License Exception NAC eligibility to include ECCN 3A090.a.2 items designed or marketed for datacenters, where the TPP is less than 4800, would benefit manufacturers of lower performance high density items which are now subject to this licensing requirement, while not surpassing a performance level that has been determined to be appropriate for additional control. For an IC with a TPP of less than 4800, whether or not designed or marketed for use in datacenters, there does not appear to be a national security concern for a performance density figure at or above 5.92, and therefore BIS should make License Exception NAC available for ECCN 3A090.a.2 items.

Request for Comment No. 6: Definition of Headquartered Companies

Without further guidance, the concept of "headquarters" is difficult to apply because of variation in how companies characterize their global offices. For example, some companies claim to have multiple headquarters or no headquarters. Other companies may be joint ventures and have two independent parent company structures with different headquarters. Still, other companies are ultimately owned by holding companies incorporated in a jurisdiction in which they do not have real operations. Such ambiguities would create difficulties when determining whether a license is required.

We recommend that BIS work with industry to develop FAQs on different types of corporate structures so that companies have more guidance. BIS should also provide and continually update a list of entities that meet this definition, which will allow companies to use standard screening processes to quickly identify customers subject to restrictions.

Request for Comment No. 7: Technical Parameters of a "Supercomputer"

Note 2 to the definition of "supercomputer" characterizes supercomputers in a way that already seems to exclude commercial datacenters used by, e.g., IaaS providers or commercial internet companies. However, BIS could make this even clearer by moving this portion of the note into the main text of the definition.

Other Comments

Exception for the Export of 3A090, 4A090, and .z items to Certain US Headquartered IaaS Datacenters

BIS should consider a license exception for exports of ECCN 3A090, 4A090, or .z products to countries in Country Group D:1 or D:4 (but not in D:5 or Macau), if the export is for use in an IaaS provider's datacenter under the operational control of a US headquartered company or a company headquartered in a US-allied country. Datacenters are highly secure facilities, and companies that maintain these datacenters have strong controls (not to mention incentives) to ensure that hardware is not removed

from the premises or diverted for uses other than in providing IaaS services. Thus, exports to datacenters in these countries do not present the same risks of diversion to D:5 countries or Macau as exports to other parties in these countries. It would be more logically consistent to address any risks associated with the hardware under whatever framework is adopted (if any) for addressing risks associated with IaaS services for training dual-use AI models. BIS provides a similar structure for authorizing exports of certain encryption items in License Exception ENC in Part 740.17 of the EAR.

Scope of the Temporary General License (TGL)

The TGL provides authorization for limited supply chain related end-use activities (integration, assembly (mounting), inspection, testing, quality assurance, and distribution) but does not appear to cover customer support. Given that some US headquartered companies may have customer support teams located in countries that require export licenses (Vietnam, China, Kuwait, etc.), it would be sensible for the TGL to authorize the transfer of products to those internal teams to support this ongoing business. Such customer support is of a similar nature to the end uses currently permitted under the TGL. Therefore, we propose the following revision in red and underlined to the end use scope of the TGL:

> *(ii) End-use scope. Any item identified under the paragraph (d)(2)(i) of this supplement, may be exported, reexported, or transferred (in-country) to or within a destination specified in Country Groups D:1, D:4, or D:5 (and not specified in Country Groups A:5 or A6) when the recipient is located in but is not headquartered or whose ultimate parent company is not headquartered in Macau or Country Group D:5 to continue or engage in integration, assembly (mounting), inspection, testing, quality assurance, ~~and~~ distribution, and customer support of items covered by items specified in paragraph (d)(2)(i) for the ultimate end use of these items outside of destinations specified in Country Groups D:1, D:4, or D:5 (and not specified in Country Groups A:5 or A6) by entities not headquartered or whose ultimate parent company is not headquartered in Macau or a destination specified in Country Group D:5.*

We also recommend that BIS clarify the ultimate end-use as referred to in the TGL. More specifically, we recommend that BIS extend the scope of the TGL to ultimate end-use in Country Groups D:1, D:4, and D:5 when the end-user is headquartered in Country Group A:5 or A:6.

Consolidation of Affected Countries

Finally, the imposition of controls based on various Country Groups (i.e., including countries in Country Groups D:1, D:4, and D:5 except for countries also included in Country Groups A:5 or A:6) creates opportunities for confusion or mistakes when making licensing determinations. We request that BIS create a positive list of countries subject to these controls in the Commerce Country Chart.

Conclusion

Thank you for your consideration of these comments and recommendations regarding the additional export controls, and we request that you implement the proposed recommendations outlined in this comment. We look forward to additional rules, and/or FAQs, addressing these points.

Sincerely,

Alliance for Network Security