Comment of the Software & Information Industry Association to interim final rule on "Implementation of Additional Export Controls: Certain Advanced Computing Items; Supercomputer and Semiconductor End Use; Updates and Corrections" (AC/S IFR)

(Docket No. 231211-0298)
(RIN: 0694-AI94)

Submitted to the Bureau of Industry and Security, U.S. Department of Commerce

January 17, 2024

On behalf of the Software & Information Industry Association (SIIA), we appreciate the opportunity to provide these comments in response to the Bureau of Industry and Security (BIS)request for comment (RFC) on interim final rule AC/S IFR (Docket No. 231211-0298).

SIIA is the principal trade association for the software and digital information industries worldwide. Our members include over 400 companies, reflecting the broad and diverse landscape of digital content providers and users in academic publishing, education technology, and financial information, along with creators of software, as well as platforms used by millions the world over.

In its request for comments, BIS states that the interim final rule seeks to advance two primary goals. First, it is imposing new export controls "to protect U.S. national security interests by restricting certain exports to China that would advance China's military modernization and surveillance efforts."[1] At the same time, BIS also acknowledges the need for a "calibrated approach" so as not to "undercut U.S. technology leadership or unduly interfere with commercial trade."[2]

SIIA agrees with the dual objectives animating the rulemaking and commends BIS for its thoughtful approach. But this is a complicated topic with regulations already in place or in the process of being implemented, some of them of recent vintage, and it is not clear how this interim final rule adds anything of import or advances the interests that BIS is pursuing. Rather than helping, duplication of authorities and the implementation of overlapping regulations likely would undermine U.S. leadership and the ability of American firms to engage in global commerce.

Question 1: Addressing access to "development" at an infrastructure as a service (IaaS) provider by customers developing large dual-use AI foundation models with potential capabilities of concern.

Cloud computing has made enormous strides in democratizing access to technology. Infrastructure-as-a-Service (IaaS) forms the backbone of the digital economy and the global technological security infrastructure. U.S. IaaS providers are global leaders in the industry, offering first-in-class products and services, strengthening U.S. national security, supporting thousands of high-skilled jobs, and helping grow our economy. But that leadership position is by no means guaranteed to

[1] 88 FR 73458.
[2] Id.

continue. China, in particular, has the largest cohort of IaaS providers outside the United States, and several European governments are working hard to foster an environment conducive to creating their own national champions.

The latter, of course, is an integral part of the European digital sovereignty agenda, which has as a central tenet the implementation of EU-wide legislation that discriminates against U.S. companies and seeks to exclude them from the EU's internal market. Examples include the Digital Markets Act, the Data Act, and the European Cybersecurity Certification Scheme for Cloud Services (EUCS).

The introduction here at home of overly broad and flexible export controls on advanced computing and semiconductor (AC/S) manufacturing items would likely exacerbate concerns in the global economy about the long-term dependence on American technology and negatively impact the global standing of U.S. IaaS providers. This would undermine not only the U.S. IaaS industry, but also U.S. national security, which is bolstered by U.S. technology leadership. Against this backdrop, we would urge BIS to proceed with great caution in this area.

In addition, the questions that BIS seeks to address in the interim final rule appear to already be covered by the President's Executive Order 14110 of October 30, 2023, on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence[3] (EO 14110), which imposes reporting and other requirements on IaaS customers and providers, as well as several of BIS' own advisory opinions.[4]

The national security objectives of the U.S. government related to AI are important, and IaaS providers undoubtedly have a role to play in seeing them fulfilled. But it is critical that the requirements imposed on these companies are consistent across regulations, and that they are realistic and practical.

For example, any controls that rely on IaaS providers knowing or providing details on the models customers are developing on their infrastructure will not be effective because IaaS providers generally do not have access to this information. Due to security, privacy, and other requirements, IaaS providers do not have access to customer workloads, and customer content is encrypted. Moreover, IaaS customers usually consider information about the volume or types of training data being used, and how they train their AI models, to be commercially sensitive and/or proprietary information. In practice, this means that they ordinarily would have wholly legitimate business reasons not to want to share this information with anyone, including the IaaS provider. And in the vast majority of cases, they do not.

In other words, requiring the IaaS provider, rather than the IaaS customer, to provide details on a customer's model, would be counterproductive because it would likely yield no responsive information and would drive customers away from U.S. IaaS providers and to foreign providers that may

[3] 88 FR 75191.

[4] *See* BIS Advisory of 1/13/09 Regarding Application of Export Administration Regulations (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; BIS Advisory of 1/11/11 Regarding Application of EAR to Grid and Cloud Computing Services: https://www.bis.doc.gov/index.php/documents/advisory-opinions/533-cloud-computing-and-deemed-exports/file; and BIS Advisory of 4/13/14 Regarding Application of EAR to Cloud-Based Storefronts: https://www.bis.doc.gov/index.php/documents/advisory-opinions/1098-cloud-based-storefronts/file

not have the same requirements or the same interests in privacy, security, or responsible AI as U.S. providers. None of this would serve U.S. national security or economic interests in any way.

In light of the above, we strongly recommend that BIS consider the following in any IaaS-related controls it may issue.

First, in accordance with existing Export Administration Regulations (EAR) and numerous BIS-issued Advisories on cloud computing, the IaaS provider is not "considered to be the "exporter" under the EAR when the user exports data store on the computational capacity or exports data resulting from use of the computational capacity."[5] Because the provider does not have visibility into the activities of its customers, the onus of submitting the required information should be on the latter.

Second, to the extent that BIS does decide to apply restrictions to IaaS providers, it should make enforcement as smooth and targeted as possible, in particular by publishing an exhaustive list of all entities that are subject to IaaS-related controls. This would provide the U.S. government with greater and more flexible enforcement capabilities, and it would help the U.S. IaaS industry maintain its global leadership position and ensure that it remains an engine of economic growth in the U.S.

Finally, in the event that BIS should decide to impose any requirements on IaaS providers, it is essential that any such restrictions apply equally to U.S. and non-U.S. providers.

Question 4: Deemed exports and deemed reexports.

Under the EAR, deemed exports and deemed reexports of AC/S are exempt from licensing requirements. This treatment has had a significant positive impact on U.S. industry and, by extension, U.S. national security, largely because it has enabled U.S. companies to recruit talent necessary to maintain global leadership in AC/S. Moreover, safeguards already exist that prevent the sort of harm that a license would seek to address.

Attracting foreign talent is critical to continued development of fields dependent on AC/S, such as AI. This is reflected in EO 14110: "Across the Federal Government, my Administration will support programs to provide Americans the skills they need for the age of AI and attract the world's AI talent to our shores—not just to study, but to stay—so that the companies and technologies of the future are made in America." Requiring a license for deemed exports and reexports will directly undermine this policy objective. It will create delays in commencing work with foreign scientists and researchers; uncertainty that will require companies to expend more resources to hedge against the chance a license will be denied or granted for a limited or secondary purpose; and uncertainty for the individual scientists and researchers. A new licensure requirement may also disrupt, if not jeopardize, currently ongoing activity in the United States.

The effects of these barriers will be significant. They will impede the ability of companies to plan and execute on projects, limiting innovation, with implications for U.S. competitiveness and the U.S. economy. They will lead top talent to seek opportunities in countries without similar restrictions, which includes foreign competitors and nations considered to be adversaries of the United States. And they

[5] *Supra* note 5 (Advisory of 1/13/09).

will turbocharge innovation in those competitor and adversary nations by creating an opportunity to attract top talent.

Moreover, existing safeguards address the core concerns underlying this proposed rule change – concerns around technology transfer, protection of intellectual property and trade secrets, and security. Companies engaged in AC/S activities have strong incentives to prevent these actions from taking place. It would undermine their economic interests were proprietary technology to be shared, leading to a range of due diligence measures and technical safeguards.

Question 5: Designed or Marketed for Datacenters

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 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.

"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,*** *or:*

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

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

Question 6: Definition of headquartered companies.

We recommend that BIS provide a brightline definition of the phrase "entities headquartered in, or whose ultimate parent company is headquartered in" to avoid ambiguity and facilitate EAR compliance. While a company headquarter denotes a physical location that may be ascertainable, determining ownership is exceedingly complex. Companies typically have multiple owners with different headquarters. Some companies may ultimately be owned by a holding company located in a different jurisdiction. Some may have a minority owner that is headquartered in a D:5 country and minority owners located in non-D:5 countries. These factors make it difficult for companies subject to the EAR to determine with certainty whether a potential counterparty meets the definition. This will lead to increased compliance costs and a risk of an unintentional EAR violation.

To address this concern, we recommend that BIS limit the definition. First, the definition should include only majority ownership by a company headquartered in a D:5 nation. Second, the definition should include guidance about the treatment of majority ownership by holding companies.

We further recommend that BIS meet and work with industry to develop practical guidance on interpreting and implementing the ultimate definition that BIS adopts.

******

SIIA thanks the BIS for considering our views. We look forward to continuing our engagement with the BIS on this important issue and would welcome the opportunity to answer any additional questions that the Bureau may have.