508.647.7000
Fax 508.647.7001
info@mathworks.com

MathWorks
3 Apple Hill Drive
Natick, MA 01760-2098 USA

www.mathworks.com

January 17, 2024

Bureau of Industry and Security
U.S. Department of Commerce
14th Street and Pennsylvania Avenue, NW.
Room 3898
Washington, D.C. 2023

By electronic submissions: www.regulations.gov

ID: BIS-2022-0025; RIN: 0694-AI94

RE: Implementation of Additional Export Controls: Certain Advanced Computing Items; Supercomputer and Semiconductor End Use; Updates and Corrections

Dear Sir or Madam:

The MathWorks, Inc. ("MathWorks") welcomes and appreciates the opportunity to submit this comment to the Bureau of Industry and Security ("BIS") on the Interim Final Rule (the "Rule")[1] concerning the implementation of additional export controls targeting advanced computing, supercomputer and semiconductor end uses.

MathWorks hereby offers the following comments for BIS's consideration in response to Request No. 1 of Section D of the Rule (the "Request for Additional Comments").

I. Summary

MathWorks understands the mission that BIS is tasked with and appreciates that certain export controls on advanced computing, supercomputer and semiconductor end uses are necessary to bolster and support U.S. national security interests. MathWorks wholly supports that mission.

As BIS acknowledges throughout the Rule, the effectiveness of the Rule—indeed, as we demonstrate below, the effectiveness of U.S. export controls more broadly—is directly undermined by the uneven application of such controls to the various modes of software and technology delivery. Namely, while U.S. export controls apply to the delivery of downloadable, on-premises proprietary software and physical hardware deliveries, they largely do not apply to the delivery of *the same* software and technology through "as-a-service" delivery models (or open source software). We share BIS's concern that such an uneven implementation of export controls creates a dangerous gap in U.S. national security,

[1] Implementation of Additional Export Controls: Certain Advanced Computing Items; Supercomputer and Semiconductor End Use; Updates and Corrections 88 Fed. Reg. 73458 (October 25, 2023).

while simultaneously eroding competitive advantages that U.S. businesses like MathWorks have assiduously developed and maintained for decades through billions of dollars in independent research and development.

As set forth below, MathWorks' comment addresses the following concerns:

- Under current U.S. export control policy, while foreign parties may be restricted from downloading and installing certain software or obtaining certain physical hardware, such parties can obtain the same or substantially equivalent technology from U.S. companies through various "as-a-service" delivery mechanisms—i.e., software-as-a-service ("SaaS," whereby such foreign parties can access and use software over the internet without downloading or installing the software), infrastructure-as-a-service ("IaaS," whereby such parties can access compute, storage, and networking resources, as well as SaaS, on-demand without the need for any physical servers or datacenter infrastructure), and platform-as-a-service ("PaaS," whereby such parties can access a complete development and deployment environment over the internet, including the same infrastructure access as IaaS, as well as middleware, development tools, business intelligence services, database management systems, and more).[2]

- While foreign parties of concern – specifically parties on the Entity List – may be restricted from procuring EAR-controlled integrated circuits, computers, servers, and software, those same entities are generally unfettered to subscribe to, access, and utilize the same capabilities through these "as-a-service" models.

- Given the widespread availability of SaaS and IaaS technologies, the lack of a clear regulatory standard subverts U.S. economic, national security, and export control interests.

MathWorks recognizes that BIS's request for comment seeks input concerning access to "development" through IaaS "*by customers to develop or with the intent to develop large dual-use AI foundation models*." Nevertheless, MathWorks respectively submits that developing a baseline framework for control for software and technology *without regard to delivery mechanism* is a fundamental threshold requirement that BIS needs to address first, before BIS can consider and impose *ad hoc* controls on AI-specific activities. As follows, MathWorks does *not* seek additional end-user or end-use controls, nor does MathWorks seek to impose burdens on U.S. providers of "as-a-service" software or technology that are not already imposed upon U.S. companies that provide the same software and technology through traditional delivery mechanisms—instead, MathWorks seeks only a level playing field.

It is in this spirit that MathWorks submits this public comment.

II. Background on MathWorks

MathWorks is a U.S. company, headquartered in Natick, Massachusetts. It develops the world's leading software for technical computing, modeling, and simulation for science, engineering, and research and development. In addition to its core products, MATLAB and Simulink, MathWorks produces over 100 other products with additional general-use functionality, such as data analysis, image processing, and visualization of automated driving scenarios.

[2] For purposes of brevity, this comment addresses SaaS and IaaS, but the same arguments supporting U.S. export control regulation apply to PaaS, as well.

MathWorks develops, markets, and licenses these products to companies and users in over 100 countries on all seven continents. Its customers include more than 5,000,000 scientists, engineers, and students, who are associated with more than 100,000 technology companies, research labs, financial institutions, and universities worldwide. This global network has helped build MathWorks software into a worldwide technology ecosystem comprised not only of MathWorks software products, but also of hundreds of third-party products based on MathWorks software.

MathWorks' software is classifiable under EAR99 and, in some cases, under ECCN 5D992, and, as such, the end user and end-use based controls that have proliferated within the EAR over the past decade have affected MathWorks.

III. Request for Comment:

Addressing access to ''development'' at an infrastructure as a service (IaaS) provider by customers to develop or with the intent to develop large dual-use AI foundation models with potential capabilities of concern, such as models exceeding certain thresholds of parameter count, training compute, and/or training data.

Pursuant to the 2018 Export Control Reform Act ("ECRA"), Congress gave BIS, acting on behalf of the U.S. Department of Commerce, broad authority to enact export control regulations. Most pertinently, ECRA enables *and requires* BIS to regulate exports to "protect United States technological advances by prohibiting unauthorized technology transfers to foreign persons . . . particularly with respect to countries that may pose a significant threat to the national security of the United States."[3] ECRA requires BIS to regulate exports "without regard to the nature of the underlying transaction or any circumstances pertaining to the activity."[4] As follows, this authority empowers—indeed, obligates—BIS to regulate the export of software and technology *without regard to delivery mechanism*, particularly when such exports are made to Entity List, Unverified List, or Military End User List entities or otherwise pose a threat to U.S. national security.

SaaS, in simple terms, is a software delivery mechanism whereby end-users access software products online via a subscription, rather than downloading and installing them on-premises on a computer or similar machine. For example, an end-user outside the U.S. may access and use a SaaS product's functionality via a web browser to operate the underlying software, which runs on an independent server sitting in the U.S. or a server provided by an IaaS provider. While the underlying software may not leave the U.S., the SaaS product that is made accessible outside the U.S. (e.g., through a web browser) contains the same graphical user interfaces ("GUIs") and other features and functionality as found in downloadable software. Today, in addition to providing direct access to compute, storage, and network resources, IaaS also serves as the backbone supporting the entire SaaS ecosystem and is quickly emerging as the primary delivery mechanism for SaaS and related capabilities.

BIS can regulate both SaaS products and IaaS under ECRA and the EAR. Especially when it comes to technical computing software offered via SaaS, the user's data is processed by the application and technical information in the form of results are returned to or exported to the user. Surely, such results are "technology" and SaaS providers are not allowed under the EAR to export such technology

[3] 50 U.S.C. 4812(b)(5).
[4] 50 U.S.C. 4812(c).

to Entity Listed users.[5] BIS has acknowledged this, finding that "there may be export of technology" when a user "utilize[s] the software application, including all its features and functions, in the cloud, without downloading the product."[6] But, BIS guidance and administration on the subject has been unclear and uneven and has left industry with the prevailing view that SaaS, and, by analogy IaaS, are not regulated by the EAR.

For example, over a decade ago, BIS publicly took the position that SaaS providers are not the "principal party in interest," and therefore cannot be "exporters" under the EAR, because end-users "receive the primary benefit" of their data stored in the cloud.[7] However, again, this is not consistent with ECRA, the EAR, or common practice today. The SaaS provider has the ability to "determine and control" the "sending" of such "technology" out of the U.S as such technology often is literally hosted on servers the SaaS provider controls.[8] And, SaaS providers have benefitted greatly from such transactions—according to one report, the global SaaS market was valued at $165.9 billion in 2021, and nearly all the largest SaaS providers are U.S. companies.[9] Clearly, SaaS providers are receiving the "primary benefit" from exporting this technology, so the only reasonable conclusion is that SaaS providers have become "exporters" under the EAR.

As noted above, IaaS can serve as a delivery mechanism for SaaS products where the SaaS provider does not host the technology on its own servers, much like a freight forwarder or common carrier. While not always the "exporter of record", BIS has routinely penalized freight forwarders and common carriers for "causing", "aiding" or "abetting" unauthorized exports. Because the delivery of SaaS products to end-users outside the U.S. constitutes an "export" of "technology," and SaaS providers are the "exporters," BIS can—indeed, must—regulate both these items *as well as* IaaS when it serves as the mode of delivery.

It is worth noting that, at the time of the 2009 Advisory Opinion, the Entity List took up 14 pages in the Code of Federal Regulations. Today, the Entity List takes up 308 pages.[10] Indeed, in this time, much of the emphasis and architecture of export regulations has changed. Now, substantial exports of EAR99 or otherwise lightly controlled software, hardware and technology are restricted—for companies like MathWorks. Yet, SaaS and IaaS providers continue to deliver the equivalent functionality of such software, hardware and technology to 308 pages worth of end users. If exports of EAR99 software, hardware and technology to certain end users threatens our national security, then so too does the export of equivalent functionality "as a service." It's time to address this unlevel playing field for industry.

---

[5] ECRA broadly defines "technology" to include "information, in tangible or intangible form, necessary for the development, production, or use of an item." 50 U.S.C. 4801(11). Moreover, the functional elements described above (e.g., GUIs and other features and functionality) are "information" transmitted to end-users through electronic and visual media (e.g., web browsers connected to the internet), and this information is necessary for users to "use" and "operate" the underlying software, thus providing another basis to conclude that IaaS and SaaS delivery models necessarily implicate exports of technology.

[6] *See* BIS Advisory Opinion, November 13, 2014.

[7] *See* BIS Advisory Opinion, January 13, 2009; see also BIS Advisory Opinion, January 11, 2011 (BIS finds that even where "technology" subject to the EAR is stored in the cloud, the provider of the cloud is not responsible for its export or deemed export because it is not the exporter. These opinions overlook that the providers of SaaS are, in fact, making exports of technology by allowing foreign nationals or persons abroad to access technology from their platforms).

[8] *See* 15 C.F.R. 772.1 (definition of exporter).

[9] https://www.grandviewresearch.com/industry-analysis/saas-market-report

[10] Based on the traditional published version of the C.F.R., available at, https://www.govinfo.gov/content/pkg/CFR-2023-title15-vol2/pdf/CFR-2023-title15-vol2-part744.pdf.

When it comes to both SaaS products and IaaS, BIS need not make any changes to existing regulations to adequately safeguard U.S. national security interests. It can revise, revoke, or reissue certain Advisory opinions and issue guidance to make clear to industry that information delivered to users of SaaS and IaaS products is "technology," even if EAR99, and that allowing access to that information from outside the United States (e.g., through web-based browsers) via an IaaS is an "export," "reexport," or "transfer," as the case may be. This simple clarification as to the administration of the EAR would close a significant gap in U.S. export controls, particularly as to SaaS and IaaS customers that are Entity List parties to which even the export of EAR99 technology is prohibited.

BIS could also amend the EAR using the "is informed" mechanism or further expansion of Section 744.6 to leverage U.S. person restrictions to ensure that proscribed parties cannot access the same type of functionality that they are prohibited from procuring in the form of the underlying hardware or software. In the January 13, 2009, BIS Advisory Opinion, the agency confirmed that SaaS providers are subject to the restrictions of Section 744.6, but it has not made clear the obligations of providers, and as currently constituted Section 744.6 does not restrict software functionality being delivered to Entity List parties absent some "knowledge" of certain particular uses. Use of the "is informed" mechanism is a means to effect controls on these types of services.

Ultimately, MathWorks urges a broad-based approach. In other words, the restrictions should go beyond the particularized controls set out in Section 744.6 today to instead prohibit any functionality, even EAR99 or 5D992-level functionality, from being delivered as a service when it cannot be delivered as on-premises software or hardware to the same end user or for the same end use. This would not only enhance U.S. national security and level the playing field for all members of industry, it would also rationalize end user and end use restrictions, which will ultimately engender respect for and adherence to the rule of law. To be clear, MathWorks does not seek additional end user and end use-based controls and urges caution by BIS in the continued proliferation of such controls to ensure the necessarily resulting losses of business for U.S. companies and developers are necessary due to *bona fide* national security risks. But where that is the case and where BIS must impose restrictions, it should do it even handedly across all distribution models.

* * *

BIS's disparate treatment of SaaS products and IaaS, as opposed to their traditionally delivered software hardware and equivalents, is not only inconsistent with its own statutory mandate to enact export controls to protect U.S. national security interests without damaging the competitiveness of U.S. companies or their leadership in science, technology, and engineering,[11] it also has become outdated to the point of abandoning a large portion (if not most) of BIS's authority over the software and cloud computing industries, including, but not limited to, advanced computing with the capacity to develop large dual-use AI foundation models with potential capabilities of concern. The unlevel playing field BIS has created harms leading U.S. innovators like MathWorks while advantaging certain other U.S. industry participants as well as many Chinese companies that utilize "as-a-service" capabilities to develop competing, China-based applications.

[11] *See* 50 U.S.C. 4811.

MathWorks respectfully submits that uneven and piecemeal regulation is detrimental to business, national security, and the rule of law. Before establishing targeted controls on "large dual-use AI foundation models *with potential capabilities of concern*," BIS must first define what "potential capabilities of concern" is intended to mean and establish a framework for placing the "as-a-service" distribution model on the same footing as traditional methods of delivery.

Respectfully submitted,

/s Thomas M. Spera
General Counsel
The MathWorks, Inc.