Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

January 17, 2024

Uploaded to https://regulations.gov at BIS-2022-0025

Thea D. Rozman Kendler
Assistant Secretary for Export Administration
Bureau of Industry and Security
U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, D.C. 20230

Subject: **Microsoft Corporation's Comments on the Interim Final Rule on Implementation of Additional Export Controls: Certain Advanced Computing Items; Supercomputer and Semiconductor End Use; Updates and Corrections [Docket Nos. 231211-0298, 231013-0248]**

References: 88 Fed. Reg. 86821, RIN 0694-AI94, Docket No. 231211-0298
88 Fed. Reg. 73458, RIN 0694-AI94, Docket No. 231013-0248

Dear Assistant Secretary Kendler:

Microsoft Corporation ("Microsoft") appreciates the opportunity to comment on the Interim Final Rule issued by the Commerce Department's Bureau of Industry and Security ("BIS") on Implementation of Additional Export Controls: Certain Advance Computing Items; Supercomputer and Semiconductor End Use; Updates and Corrections published in the Federal Register on October 25, 2023 ("the AC/S Rule" or "the Rule"). Microsoft recognizes and appreciates the national security implications associated with advanced semiconductors and supercomputers and supports a careful approach to controlling these items in a manner that does not stifle innovation.

As a leading technology company, Microsoft has long devoted significant resources and personnel to developing and advancing defensive security measures designed to protect software, data, and systems against the growing threat of malicious cyber actors. These activities are vital for securing Microsoft's own networks and products, Microsoft's customers around the world, and, more broadly, the U.S. information technology infrastructure.

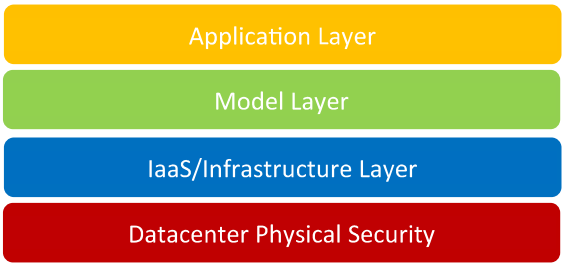
As we have expanded our work in Artificial Intelligence ("AI"), particularly our work with advanced generative AI models, security has become even more essential. As the technology

progresses, it is just as important that we ensure proper control over AI as it is to pursue its benefits. We are committed and determined as a company to develop and deploy AI in a safe and responsible way. Today's highly capable AI models are built on advanced AI datacenters. They require huge amounts of computing power, specialized AI chips, and sophisticated infrastructure engineering. As BIS has rightly identified, such AI datacenters are therefore critical enablers of today's highly capable AI models and one effective control point in a comprehensive regulatory regime.

To that end, BIS asked for comments from Infrastructure as a Service ("IaaS") providers and other stakeholders on additional regulations that may address national security concerns relating to the development of frontier AI models. BIS expressed particular interest in "know your customer" requirements that can be adopted to address AI uses that present national security or foreign policy concerns. Microsoft focused its comments on this request and offers below suggestions on how such controls could be implemented to effectively ensure security of IaaS offerings and to better target nefarious uses of AI infrastructure and ultimately AI models.

I. Overview

When thinking about the development and security of frontier AI models, infrastructure providers and model developers must consider all potential vectors of compromise, starting at the layer of datacenter physical security and continuing through the application layer. BIS has an opportunity to ensure certain safety measures at the IaaS/Infrastructure layer through its authorities under export control laws and Executive Order 13984 of January 19, 2021, Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities ("the IaaS EO"). As described below, Microsoft supports (1) the imposition of certain cybersecurity best practices at the infrastructure level and (2) more traditional Know Your Customer ("KYC") elements and reporting requirements for access to advanced datacenter chips.



Such best practices and requirements foster a hardened infrastructure less susceptible to malicious actors. They ensure that IaaS providers have measures that discourage misuse of the advanced datacenter chips that are the subject of the AC/S Rule ("Advanced AI Chips") and that mitigate concerns about nefarious uses of large amounts of compute power.

To the extent that BIS is also considering imposing restrictions on access to Advanced AI Chips, BIS should focus restrictions on specific end users of concern, such as Military End Users ("MEUs") and Entity Listed Entities. Broader country-based prohibitions, such as a rule prohibiting all Chinese companies from remotely accessing these Advanced AI Chips, would be more encompassing than necessary to address the national security threat.

II. Commerce Should Require IaaS Providers Receiving Advanced Chips to Have Certain Cybersecurity Best Practices in Place

At a fundamental level, IaaS operators offering customers remote access to Advanced AI Chips must have in place certain cybersecurity best practices designed to identify malicious actors

on their network. Such a requirement establishes a necessary, base layer of security in the AI ecosystem. Commerce is uniquely positioned to leverage both its export control authorities and its authorities under the IaaS EO to impose such cybersecurity best practices on both domestic and foreign IaaS providers offering access to Advanced AI Chips. Microsoft describes below critical cybersecurity best practices and offers ways to incorporate those best practices into BIS's export licensing policy.

A. Best Practices for Deterring Abuse of IaaS Services

Microsoft recommends that BIS, under the IaaS EO, require U.S. IaaS providers offering access to Advanced AI Chips to meet the following cybersecurity best practices. Similarly, under export control licensing policies, BIS should require foreign IaaS providers that import Advanced AI Chips to implement the cybersecurity best practices. Specifically, these IaaS providers must:

1) Establish and enforce terms of service that clearly prohibit malicious cyber activity and detail actions to be taken in response to activity found to be in violation of those terms.
2) Provide means and instructions for third parties to easily report suspected or confirmed abuse and monitor and act on such reports in a timely manner.
3) Maintain a compliance program and established policies and practices for addressing government requests for data associated with law enforcement investigations, in accordance with relevant data privacy requirements.
4) Implement account creation and resource allocation processes to mitigate the risk of fraud.
5) Document, maintain, and implement internal policies and procedures for detecting, mitigating, and responding to abuse, including by:
    a. Establishing steps to identify and evaluate accounts suspected of conducting malicious activity, fraud or abuse;
    b. Implementing steps to mitigate the offending behavior such as via restricting account access to new resources, requiring further proof of legitimacy, and/or removing resources engaged in malicious activity.
    c. Establishing metrics for reducing abuse and continually measuring performance against them.
6) Prohibit the use of payment instruments for IaaS services that can increase anonymity, including by prohibiting the use of crypto currency to procure services except when using accredited third-party platforms subject to financial know-your-customer requirements.
7) Ensure that reseller channels are not used to facilitate abuse, including by:
    a. Monitoring reseller compliance with terms of service.
    b. Notifying resellers when their customers are detected abusing services.
    c. Holding resellers accountable if a pattern of abuse is detected by its customers.
8) Collaborate in cross-industry and government efforts to deter abuse, including by:
    a. Increasing technical information sharing and cooperation through existing inter-company mechanisms and dedicated trust groups.
    b. Participating in collaborative efforts between IaaS providers and government that facilitate the sharing of cyber threat information to enable collective cyber defense.

Microsoft notes that these best practices should not be static. Best practices should be updated as malicious actors change their attack methods. As reflected in 8(b) above, two-way information sharing of cyber threat information between government and industry is critical to ensuring that

security practices evolve to address the threat. Indeed, recommendation number two in the September 19, 2023 National Security Telecommunications Advisory Committee (NSTAC) Report ("NSTAC Report") recommends such a committee for sharing this type of information.

B. BIS Should Impose These Best Practices Pursuant to the IaaS EO and as Part of its AC/S Licensing Policy

Microsoft recommends that BIS impose these cybersecurity best practices as part of its authorities under the IaaS EO and export control laws. Under the IaaS EO, BIS could require all U.S. IaaS providers offering access to the Advanced AI Chips to have these cybersecurity best practices in place.[1] Microsoft recognizes that the structure of the IaaS EO calls for mandatory KYC requirements for all IaaS providers, and allows the Secretary of Commerce to exempt from those requirements IaaS providers meeting certain safety standards. The cybersecurity best practices recommended in these comments could be used to qualify IaaS providers for the exemption. Alternatively, for the reasons described in the NSTAC Report, Microsoft recommends the Administration consider revising E.O. 13984 to focus on cybersecurity best practices, which are much more successful than traditional KYC data points in identifying, deterring, and disrupting malicious cyber conduct, but additionally impose KYC requirements, as described below, for certain advanced IaaS offerings.

Microsoft also recommends that, as part of the licensing process described in the AC/S Rule, BIS require foreign IaaS providers receiving the Advanced AI Chips to certify that they have implemented these cybersecurity best practices. Specifically, whenever a license is required under the Rule, Commerce should require the exporter of record to first obtain from the foreign IaaS provider a certification that it has such cybersecurity best practices in place. Alternatively, BIS could require that the foreign IaaS provider file that certification directly with BIS. For those countries for which no license is required for the export of the Advanced AI Chips, BIS should work with those governments to impose similar cybersecurity best practice mandates.

These Advanced AI Chips are powerful and warrant cybersecurity measures commensurate with their capabilities. IaaS providers hosting these chips and offering access to them remotely should embrace these practices and recognize them as fundamental aspects of a secure cyber infrastructure.

III. BIS Should Require Standard KYC Requirements for Customers Accessing a Certain Amount of Compute

As part of its AI Governance Blueprint, Microsoft recommended a know your cloud and know your customer approach for frontier AI models as well as users of a high amount of AI model development-enabling cloud infrastructure. Under such KYC principles, it is incumbent on AI infrastructure providers to know their customers that have access to compute resources sufficient to develop highly capable models. BIS should consider a requirement that such infrastructure providers impose a gating mechanism, requiring the provider to collect additional KYC

[1] While Microsoft makes these recommendations in the context of IaaS providers offering access to Advanced AI chips, Microsoft also recommends that BIS apply the recommendations for IaaS/cloud service providers hosting frontier AI models.

information about users developing a highly capable model. To date, one input for anticipating a model's capability has been the amount of compute power accessed for model training. While Microsoft is not recommending a particular level of compute power – and while we recognize it is an ongoing process to define more robust and durable methods for determining whether models should be considered highly capable or as presenting potentially dangerous capabilities – we also note near-term efforts to leverage a compute threshold as a rough indicator in the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence ("AI EO"). BIS should align the compute threshold that triggers KYC requirements with the level of compute that the Department of Commerce uses pursuant to the AI EO (the "Identified Level of Compute"). Again, BIS can rely on its authorities under the IaaS EO and export control laws to require domestic and foreign IaaS providers to comply.

A. KYC Data Points

Under this approach, when a customer seeks access to and use of the Identified Level of Compute, the IaaS provider should confirm standard KYC data points, such as those listed in the AI EO:

1) The identity of the customer, including name and address;
2) The means and source of payment (including any associated financial institution and other identifiers such as credit card number, account number, customer identifier, transaction identifiers, or virtual currency wallet or wallet address identifier); and
3) the electronic mail address and telephonic contact information used to verify a customer's identity.

The gating mechanism could also require users to describe generally the purpose of the large volume of compute, and should require customers to attest that they will not use the chips for certain malicious purposes. IaaS providers should maintain records of this information for a period of five years after the customer ceases using the service.

B. BIS Could Use Its Authorities Under the IaaS Rule and Export Control Laws

Under the IaaS EO, BIS has the authority to impose KYC requirements on U.S. IaaS providers. Instead of a broad-based requirement for all IaaS services that IaaS providers offer, however, the Administration should consider limiting the KYC requirements to certain advanced services, such as offering access to the Identified Level of Compute – allowing IaaS providers to implement cybersecurity best practices in lieu of KYC requirements for other IaaS uses. Under such a requirement, U.S. IaaS providers would collect and maintain KYC information related to users of the Identified Level of Compute.

Similarly, under the AC/S Rule, Commerce could require foreign recipients of Advanced AI Chips to collect and maintain these KYC data elements for the Identified Level of Compute in order to obtain the chips. Under this requirement, before procuring an export license under the AC/S Rule, exporters of record would need to obtain certifications from foreign IaaS providers that those foreign providers will collect, retain, and make available for BIS inspection the KYC

information for users of the Identified Level of Compute. Alternatively, BIS could require foreign IaaS providers to file that certification directly with BIS.

Ideally, BIS would impose these requirements in coordination with allies. Allies would impose the same or similar KYC requirements on IaaS providers operating in their countries. This coordinated approach would help mitigate the risk that customers move away from U.S. IaaS providers because they are reluctant to provide this KYC information.

IV. Restrictions on "Remote Access"

Microsoft understands that BIS is considering additional restrictions on "remote access" to Advanced AI Chips. Historically, BIS has taken the position that such a "cloud service" does not involve an export and therefore is not subject to export control restrictions. Microsoft agrees with that interpretation and encourages BIS to retain that precedent. However, Microsoft understands that certain entities pose a heightened national security threat because they might access the Advanced AI Chips for weapons development or other military purposes. Microsoft encourages BIS to focus any restrictions on specific entities of concern, such as Entity Listed entities and MEUs, in lieu of broad country-wide prohibitions. A broad ban is more encompassing than necessary to address the national security threat.

For these reasons, Microsoft recommends that BIS limit any "remote access" restrictions to entities of concern, specifically, MEUs, Entity Listed entities, and entities on the unverified list.

V. Conclusion

Microsoft appreciates BIS's request for comments on the AC/S Rule and welcomes the opportunity to engage with BIS on ways to identify and prohibit nefarious uses of IaaS infrastructure, particularly the Advanced AI Chips. If you have additional questions or would like to discuss further, please contact Sarah O'Hare O'Neal, Deputy General Counsel, at Sarah.ONeal@microsoft.com or (202) 365-9011.

/s/ Sarah O'Hare O'Neal
Sarah O'Hare O'Neal
Partner, Associate General Counsel, Global Trade
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052