Now & Next

Export Controls Alert

January 31, 2024

Overview of the new rules regulating Infrastructure as a Service

By Jule Giegling,[1] Alexandra López-Casero, and David Crosby

The proposed requirements include customer identification verification and foreign reseller requirements.

What's the impact?

- The Proposed IaaS Rules are part of a recent trend toward regulating critical technologies that could threaten the national security of the United States.
- The proposed rules could have a chilling effect on U.S. IaaS providers—DOC is accepting public comments through April 29, 2024.

On January 29, 2024, the U.S. Department of Commerce (DOC) published a Notice on Proposed Rulemaking (the Proposed IaaS Rules), which seeks to establish new requirements for Infrastructure as a Service (IaaS), including customer identification verification, the implementation of a written Customer Identification Program, and foreign reseller requirements. These new Proposed IaaS Rules are not yet effective. The DOC has solicited comments from industry, which must be received by April 29, 2024. These proposed regulations implement

[1] Jule Giegling (Legal Intern—Corporate Practice) assisted with the preparation of this alert.

Executive Orders issued by the Obama, Trump, and Biden administrations, especially Executive Orders 13984 and 14110, with which the Biden-Harris administration aims to address the potential national security risks associated with frontier AI models and the abuse of U.S. cloud infrastructure by malicious cyber actors.

Purpose of the Proposed IaaS Rules

The Proposed IaaS Rules are part of various recent and new controls that regulate critical technologies considered to have the potential to threaten the national security of the United States, such as the ''Implementation of Additional Export Controls: Certain Advanced Computing Items; Supercomputer and Semiconductor End Use; Updates and Corrections,'' and ''Export Controls on Semiconductor Manufacturing Equipment,'' which became effective on November 17, 2023.

The Proposed IaaS Rules will not be incorporated in the Export Administration Regulations; instead, they will be in a separate set of regulations, specifically, Subpart D to 15 CFR Part 7, consisting of §§ 7.300 through 7.310. The Proposed IaaS Rules require U.S. IaaS providers (as defined below) of U.S. IaaS products to implement a written Customer Identification Program (CIP), as explained below, to maintain specific records related to IaaS accounts in which foreign persons have an interest. The regulatory and enforcement authority for the new rules lies with the DOC.

What is a U.S. IaaS provider?

The Proposed IaaS Rules defined the term ''U.S. IaaS provider'' as any U.S. person that offers IaaS products. The DOC clarifies, in comments preceding the actual rules, that this includes both direct providers of U.S. IaaS products and any of their U.S. resellers. A U.S. IaaS product means a product or service offered to a consumer, including complimentary or ''trial'' offerings, that provides processing, storage, networks, or other fundamental computing resources and with which the consumer is able to deploy and run software that is not predefined, including operating systems and applications.

The DOC explains that the consumer typically does not manage or control most of the underlying hardware but has control over the operating systems, storage, and any deployed applications. It further elaborates that the term is inclusive of ''managed'' products or services in which the provider is responsible for some aspects of system configuration or maintenance and ''unmanaged'' products or services in which the provider is only responsible for ensuring the product is available to the consumer. The term is also meant to be inclusive of ''virtualized'' products and services, in which the computing resources of a physical machine are split between virtualized computers accessible over the internet (e.g., ''virtual private servers''), and ''dedicated'' products or services in which the total computing resources of a physical machine are provided to a single person (e.g., ''bare metal'' servers).

Customer Identification Program Requirements

Each U.S. IaaS provider must ensure that each foreign reseller of its U.S. IaaS product itself maintains and implements a written CIP. A "foreign reseller" is defined as any foreign person that has established an account with a U.S. IaaS provider to provide IaaS products subsequently, in whole or in part, to a third party.

The CIP must, as a minimum, not only include the full name, address, means and source of payment, and the IP address used for access or administration of each foreign customer but, for entities, also the principal place of business, the jurisdiction under whose laws the entity is constituted or organized, and notably the name(s) of the beneficial owner of the account. A beneficial owner is an individual who either exercises substantial control over a customer or owns or controls at least 25% of the ownership interests of a customer. The minimum requirements for the CIP are detailed in the Proposed IaaS Rules (§ 7.302(a)). Each U.S. IaaS provider must notify the DOC of the implementation of its CIP and, if relevant, the CIPs of each foreign reseller of its U.S. IaaS products through submission of a CIP certification form, which will include information on the mechanisms, services, software, systems, or tools the IaaS provider uses to verify the identity of foreign persons, the procedures the IaaS provider uses to require a customer to notify the IaaS provider of any changes to the customer's ownership, and the process for ongoing verification, the number of IaaS customers, the number and locations of the IaaS provider's foreign beneficial owners, a list of all foreign resellers of IaaS products, and the number of IaaS customer accounts held by foreign customers whose identity has not been verified (§7.304). They further must submit to the DOC certifications of their CIPs on an annual basis and, if relevant, the CIPs of each foreign reseller of its U.S. IaaS products (§ 7.302(b)).

The Proposed IaaS Rules provide for an exemption of the CIP requirements for any U.S. IaaS provider, specific type of account or lessee, or any specific foreign reseller of a U.S. IaaS provider's IaaS products from the CIP requirements if the DOC determines that the person has implemented best practices to otherwise deter abuse of their products (§7.306).

Covered Transactions under Proposed IaaS Rules

Additionally, the Proposed Rules, under § 7.308, establish a reporting obligation on U.S. IaaS providers if they have knowledge—which includes not only positive knowledge that the circumstance exists or is substantially certain to occur but also an awareness of a high probability of its existence or future occurrence—of so-called "Covered Transactions" The report must be filed within 15 calendar days of a covered transaction occurring or the provider or reseller having 'knowledge' that a covered transaction has occurred. A covered transaction is a transaction:

- By, for, or on behalf of a foreign person which results or could result in the training of a large AI model with potential capabilities that could be used in malicious cyber-enabled activity, for example:

- Corporation A, a foreign person, proposes to train a model on the computing infrastructure of Corporation B, a U.S. IaaS provider, and signs an agreement with Corporation B to train the proposed model. The technical specifications of the model that Corporation A seeks to train meet the technical conditions of a large AI model with potential capabilities that could be used in malicious cyber-enabled activity.
- Corporation A, a U.S. person, makes an equity investment in Corporation B, a foreign person, and a portion of that investment is in the form of credits to use Corporation A's computing infrastructure. Corporation A has reason to believe that Corporation B intends to use those credits to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity.

/ By, for, or on behalf of a foreign person, in which the original arrangements provided for in the terms of the transaction would not result in a training of a large AI model with potential capabilities that could be used in malicious cyber-enabled activity but a development or update in the arrangements means the transaction now does or could result in the training of a large AI model with potential capabilities that could be used in malicious cyber-enabled activity, for example:

- Corporation A, a U.S. person, agrees to train an AI model for Corporation B, a foreign person. At the outset, the agreed-upon technical specifications for the model do not meet the technical conditions of a dual-use foundation model or a model with technical conditions of concern. However, after training commences, adjustments in the training procedure or new insights about the model's capabilities provide Corporation A with reason to believe that the model will, in fact, have the technical conditions of a large AI model with potential capabilities that could be used in malicious cyber-enabled activity.

A large AI model with potential capabilities that could be used by foreign persons for malicious cyber-enabled activities would be identified through technical parameters of concern, which will be described in an interpretative rule.

REPORTING OBLIGATIONS FOR COVERED TRANSACTIONS

Apart from its own reports, the U.S. IaaS provider must further require a report from each foreign reseller whenever the foreign reseller has knowledge of a covered transaction. U.S. IaaS providers must require their foreign resellers to file with the U.S. IaaS provider a report within 15 calendar days of a covered transaction occurring or the provider or reseller having ''knowledge'' that a covered transaction has occurred. The U.S. IaaS provider must then file this report with the DOC within 30 calendar days of the covered transaction. The content of the reports on large AI model training must include information on the foreign person, such as the full name and address of the foreign customer or foreign beneficial owner of the customer, means and source of payment and the IP address used for access or administration, the date and time of each such access or administrative action, and information about the training run, such as the estimated number of computational operations, the anticipated start date and completion date of the training run, information on training practices, including the model of the primary AI used in the

training run accelerators and information on cybersecurity practices. The required contents of the report are detailed in §7.308(d).

DOC Special Measures under the Proposed IaaS Rules

Apart from these obligations, the Proposed IaaS Rules outline Special Measures the DOC can take if it determines that there are reasonable grounds for concluding that a jurisdiction or person outside of the U.S. has any significant number of foreign persons offering U.S. IaaS products that are used for malicious cyber-enabled activities or any significant number of foreign persons directly obtaining U.S. IaaS products for use in malicious cyber-enabled activities (§7.307). For this determination, the DOC can initiate investigations of its own accord or accept referrals from other executive branch agencies or providers. The DOC would be allowed to prohibit or impose conditions on the opening or maintaining of an account, including a reseller account, by any foreign person located in a foreign country or by any U.S. IaaS provider of U.S. IaaS products for or on behalf of a foreign person.

IaaS Enforcement Protocols

Violations of the Proposed IaaS Rules may be followed by civil or criminal penalties under the IEEPA. The Proposed IaaS Rules further create a new enforcement section specific to violations of IaaS-specific provisions (§7.309). For example, the new enforcement section specifies that it is a violation to fail to create a CIP, file a CIP certification with the DOC, or seek reauthorization for such CIPs on an annual basis. It is also a violation to fail to inform the DOC about a covered IaaS transaction that might result in a customer obtaining or using a large AI model with potential capabilities that could be used in malicious cyber-enabled activity when a IaaS provider knows or should know of such a transaction.

BIS Seeking Public Comments Regarding Proposed IaaS Rules

As noted above, BIS is seeking public comments on all aspects of the Proposed IaaS Rules until April 29, 2024. In light of their potential broad scope and the chilling effect these rules could have on U.S. IaaS providers, we recommend those potentially affected by these rules review them thoroughly and participate in the commentary process.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Alexandra López-Casero
202.213.0171
alopezcasero@nixonpeabody.com

David F. Crosby
617.345.1264
dcrosby@nixonpeabody.com