Know Your Cloud Customer: Commerce Department Proposes To Regulate Foreign Access to US IaaS Products

Skadden

February 13, 2024

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

One Manhattan West
New York, NY 10001
212.735.3000

1440 New York Ave., N.W.
Washington, D.C. 20005
202.371.7000

On January 29, 2024, the Department of Commerce, Bureau of Industry and Security (BIS) released a proposed rule (Proposed Rule) that would require U.S. cloud services providers (a.k.a. Infrastructure as a Service, or IaaS, providers) to create sweeping new programs to identify, assess and track foreign customers of their IaaS products.

The Proposed Rule also authorizes BIS to prohibit or impose conditions on IaaS transactions in jurisdictions, or with specific foreign persons, found to have engaged in cybersecurity-related abuse of U.S. IaaS products (Special Measures). Finally, the Proposed Rule would require U.S. IaaS providers to submit reports to BIS when foreign customers use U.S. cloud computing services to train large artificial intelligence (AI) models with potential use in malicious cyber-enabled activity (AI Reporting).

The Proposed Rule, which BIS promulgated pursuant to cybersecurity-related Presidential emergency authorities,[1] will not be finalized for at least several months. Comments on the proposal are due April 29, 2024, and we anticipate that BIS will require significant additional time to consider comments before finalizing the regulations.

BIS separately has indicated that it is considering changes to U.S. export controls (which it also administers) that would impact cloud-service providers. Thus, the Proposed Rule may be only one of multiple initiatives undertaken by BIS to regulate the provision of cloud computing services by U.S. companies.

What Is IaaS and Who Are U.S. IaaS Providers?

The Proposed Rule, which applies to "U.S. IaaS providers," defines IaaS as "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."

BIS indicates that it considered numerous comments before arriving at this definition, some of which requested a broad term "to capture as much potential foreign malicious cyber activity as possible," while others argued that BIS should "avoid implicating cloud service providers who offer other cloud-based services, such as Platform as a Service (PaaS) and Software as a Service (SaaS) offerings, but do not offer IaaS products." The definition in the Proposed Rule appears to fall somewhere in the middle of these two extremes.

"U.S. IaaS providers" include any U.S. person, including U.S. subsidiaries of foreign entities, that sell IaaS products, and U.S. resellers of such products. While foreign subsidiaries of the U.S. IaaS providers are not included in the definition, U.S. IaaS providers need to ensure their foreign resellers implement CIP requirements.

[1] The Proposed Rule implements cybersecurity-related authorities delegated to the Commerce Department in Executive Order (E.O.) 13984 ("Taking Additional Steps to address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities") issued by President Trump in January 2021, and E.O. 14110 ("Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence") issued by President Biden in November 2023. These E.O.s were issued pursuant to the President's emergency authorities under the International Emergency Economic Powers Act (IEEPA).

Know Your Cloud Customer: Commerce Department Proposes To Regulate Foreign Access to US IaaS Products

Customer Identification Program Requirements

The Proposed Rule requires U.S. IaaS providers to develop and maintain a written Customer Identification Program (CIP) that establishes procedures for identifying and verifying foreign user accounts. U.S. IaaS providers have some flexibility to craft their CIP so long as it is appropriate given the IaaS provider's size, the type of products offered and related risks. The CIP must generally include the following elements:

- **Identification and verification:** The CIP must identify procedures for verifying customer identities and determining whether they are U.S. or foreign persons. The CIP must also identify remediation procedures, including closing accounts and other corrective actions, where a U.S. IaaS Provider is unable to verify a customer's identity.
- **Data collection and maintenance:** In implementing a CIP, a U.S. IaaS provider will need to establish policies to collect and maintain verification information on their foreign account holders to include name, address, means and source of payment, email address, telephone contact information, and IP addresses from any potential foreign customer or foreign beneficial owner prior to opening an account.
- **Retention and security requirements:** U.S. IaaS providers are required to retain records and data securely for up to two years after a customer account is last accessed or is closed.
- **Foreign resellers of U.S. IaaS:** Each U.S. IaaS provider must ensure that any foreign reseller of its U.S. IaaS products maintains and implements its own written CIP and must provide the foreign reseller's CIP to BIS upon request.

U.S. IaaS providers will be required to certify compliance with CIP requirements to BIS within some period of time after the Proposed Rule becomes effective, and annually thereafter. As part of their certification to BIS, U.S. IaaS providers must provide details regarding CIP implementing procedures, service offerings, unverified foreign accounts and foreign reseller compliance. Additional reporting is required for material changes to business operations or corporate structure or material changes to a U.S. IaaS providers' CIP. The Department of Commerce retains broad authority to conduct annual compliance assessments, require changes to the CIP or request an audit.

Under the Proposed Rule, BIS may exempt from the CIP requirements U.S. IaaS providers and/or their foreign resellers who maintain an "Abuse of IaaS Products Deterrence Program" (APDP program) approved by BIS designed to detect, prevent and mitigate malicious cyber-enabled activities. Among other things, APDP programs will require U.S. IaaS providers to undertake similar efforts to verify customers, monitor IaaS product use, and identify, address, and report red flags of potential malicious cyber-enabled activities.

Special Measures

The Proposed Rule would implement the authorities granted to the Secretary of Commerce in E.O. 13984 in 2021 to prohibit or impose conditions on opening or maintaining an account for:

- all users in a specific foreign jurisdiction if that jurisdiction is found to have any significant number of foreign persons offering U.S. IaaS products for malicious cyber activities, and
- specific foreign persons if those foreign persons are found to be directly supporting the use of U.S. IaaS products in malicious cyber-enabled activities.

While the scope of these authorities is broad, the Commerce Department's use of them must be tied to a determination that the underlying jurisdiction or person is using U.S. IaaS products to engage in malicious cyber-related activities.

AI Reporting Requirements

The Proposed Rule would also require U.S. IaaS providers to report to BIS any transaction with a foreign person that, based on U.S. IaaS provider's "knowledge" (including "reason to know"), either (a) could result in the training of a large AI model that could be used in malicious cyber-enabled activity or (b) where a change in scope in existing uses of U.S. IaaS products results in the training of a large AI model that could be used in malicious cyber-enabled activity.

The Proposed Rule defines "large AI model with potential capabilities that could be used in malicious cyber-enabled activity" as "any AI model with the technical conditions of a dual-use foundation model or otherwise has technical parameters of concern, that has capabilities that could be used to aid or automate aspects of malicious cyber-enabled activity, including but not limited, to social engineering attacks, vulnerability discovery, denial-of-service attacks, data poisoning, target selection and prioritization, disinformation or misinformation generation and/or propagation, and remote command-and-control of cyber operations."

The Proposed Rule indicates that the Commerce Department intends to publish further interpretive guidance on the scope of this definition. Reports to BIS will be due within 15 days of a covered transaction occurring or the provider or reseller having "knowledge" that a covered transaction has occurred. U.S. IaaS providers must apply the reporting requirement to their foreign resellers.

Know Your Cloud Customer: Commerce Department Proposes To Regulate Foreign Access to US IaaS Products

Enforcement

Failure to comply with the Proposed Rule can result in civil penalties of up to the greater of $250,000 per violation or the twice the amount of the transaction value, and criminal penalties of up to $1,000,000 per violation or up to 20 years imprisonment may be imposed.

Conclusion

The Proposed Rule, which has been in development for over two years, is part of an ambitious attempt by the Biden administration to ensure that U.S. IaaS is not used by foreign actors in a manner that is harmful to U.S. national security.

While the Proposed Rule is focused on the use of U.S. IaaS to engage in malicious cyber-enabled activities, BIS is separately seeking public comment on whether the U.S. Export Administration Regulations (EAR) administered by BIS should also be changed to regulate the provision of U.S. IaaS services to non-U.S. customers. In October 2023 BIS indicated "concern[] regarding the potential for China to use IaaS solutions to undermine the effectiveness" of the new U.S. export controls on advanced semiconductors, and that BIS "continues to evaluate how it may approach this through a regulatory response." It is possible, therefore, that BIS may propose changes to the EAR that could have an additional impact on U.S. IaaS providers.

The Proposed Rule also represents another measure taken by the administration to increase federal cybersecurity-related regulatory requirements on U.S. companies. These efforts include the new Cyber Maturity Model Certification (CMMC) program for defense contractors, and Commerce Department´s implementation of its existing authorities to regulate the information and communications technology and services (ICTS) supply chain in the United States.

Collectively, these rules aim to shore up U.S. defenses to malicious cyber-enabled activity, and to prevent U.S. companies from directly or indirectly supporting malicious cyber-enabled activities conducted overseas. AI, which is critical to advancing cyber capabilities, is likely to continue to be the focus of U.S. regulation.

Contacts

Brian J. Egan
Partner / Washington, D.C.
202.371.7270
brian.egan@skadden.com

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Tatiana O. Sullivan
Counsel / Washington, D.C.
202.371.7063
tatiana.sullivan@skadden.com

Joshua Silverstein
Counsel / Washington, D.C.
202.371.7148
joshua.silverstein@skadden.com

Andy Law
Law Clerk / Washington, D.C.
202.371.7367
andy.law@skadden.com

Sruthi Venkatachalam
Law Clerk / Washington, D.C.
202.371.7276
sruthi.venkatachalam@skadden.com