alert

U.S. Department of Commerce Publishes Proposed Rule Imposing “Know Your Customer” and Reporting Requirements on U.S. Infrastructure as a Service Providers

International Trade
February 1, 2024

The U.S. Department of Commerce (“Commerce”), Bureau of Industry and Security (“BIS”) recently issued a proposed rule aimed at preventing foreign actors from utilizing U.S. Infrastructure as a Service (“IaaS”) products (i.e., cloud computing services) to engage in malicious cyber-enabled activity, specifically by imposing certain due diligence and reporting requirements on U.S. IaaS providers and their foreign resellers. The January 29, 2024, Notice of Proposed Rule Making (“NPRM”) follows Executive Order ("EO") 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 EO 14110 (“Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence”), issued by President Biden in October 2023. BIS has invited the public to submit comments on the proposed rule by April 29, 2024.

The proposed rule, which would amend the Information and Communications Technology and Services (“ICTS”) regulations (15 C.F.R. Part 7), focuses on three central policy objectives:

1. Requiring U.S. IaaS providers and their foreign resellers to implement a Customer Identification Program (“CIP”);

2. Empowering the U.S. Department of Commerce to prohibit or restrict access to U.S. IaaS products by certain foreign persons or persons in certain foreign jurisdictions; and

3. Requiring U.S. IaaS providers and their foreign resellers to report known instances of foreign persons training large artificial intelligence models “with potential capabilities that could be used in malicious cyber-enabled activity” (e.g., social engineering attacks or denial-of-service attacks).

Customer Identification Program

The proposed rule requires all U.S. providers of U.S. IaaS products to create, implement, and maintain an appropriately tailored, written CIP—akin to the “know your customer” (“KYC”) information that banks maintain. The primary purpose of the CIP is to verify whether potential customers and

beneficial owners are foreign or U.S. persons, and to verify the identities of potential foreign customers and their beneficial owners.

1. ***CIP Identification Procedures***

At minimum, U.S. IaaS providers must gather and retain specific identifying information from potential foreign customers and foreign beneficial owners to verify their identity, including their:

- Name;
- Address;
- Means and source of payment;
- Email address;
- Telephone number; and
- "IP address(es) used for access or administration and the date and time of each such access or administrative action."

Similar to the anti-money laundering regulations administered for financial institutions under the Bank Secrecy Act, the BIS proposed rule defines "beneficial owner" as an individual who "exercises substantial control over a [c]ustomer or owns or controls at least 25 percent of the ownership interests of a [c]ustomer."

The proposed rule seems to suggest that providers should assume all potential customers and beneficial owners are non-U.S. persons until the aforementioned identifying information is collected and assessed. If a provider verifies that "the potential customer and all beneficial owners are U.S. persons," the provider need not engage in further verification procedures. (The proposed rule defines U.S. persons as U.S. citizens, U.S. lawful permanent residents, U.S.-incorporated entities and their foreign branches, and persons located in the United States.)

If, however, the provider has collected all requisite information and determined that the potential customer and beneficial owner[s] are non-U.S. persons or entities, the provider must then confirm the identity of the potential foreign customer and foreign beneficial owner through selected documentary or non-documentary identity verification procedures.

If the provider "doubt[s] the true identity of a potential [foreign] customer" and foreign beneficial owner—or cannot verify the identity of such—the provider must obtain further information, "including signatories, to verify the potential [foreign] customer's [or foreign beneficial owner's] identity."

The proposed rule also requires CIPs to outline next steps if an IaaS provider cannot verify the identity of a potential foreign customer or foreign beneficial owner. At minimum, the CIP must include:

- "When the IaaS provider should not open an account for the potential customer;"
- "The terms under which a customer may use an account while the IaaS provider attempts to verify the identity of a customer or beneficial owner of the account, such as restricted permission or

enhanced monitoring;"

- "When the IaaS provider should close an account or subject it to other measures, such as additional monitoring . . . after attempts to verify the identity of a customer or beneficial owner of the account have failed;" and

- "Other measures for account management or redress for customers whose identification could not be verified or whose information may have been compromised."

In addition, IaaS providers must retain all identifying information relied upon to verify the identity of a foreign customer or foreign beneficial owner for a period of no less than "two years after the date the IaaS account is closed or the date the account was last accessed."

To facilitate comprehensive oversight, the proposed rule also requires that CIPs include certain "risk-based procedures" requiring:

1. "Customer[s] notify the IaaS provider when the customer adds beneficial owners to its account;" and

2. "Periodic continued verification of the accuracy of the information provided [to the IaaS provider] by the customer."

The proposed rule requires U.S. providers to flow through the above requirements to their foreign resellers. If a provider becomes aware that its foreign resellers are not complying with the requirements of the rule, the U.S. IaaS provider must "terminate the reseller relationship within 30 calendar days" and "report the suspected or [known] malicious cyber-enabled activity discovered to relevant authorities."

2. ***CIP Reporting Requirements***

The proposed rule requires U.S. IaaS providers and their foreign resellers to submit a CIP certification form to Commerce detailing, in relevant part:

- A description of the identity verification procedures used by the provider;

- The resources used by the provider to detect malicious cyber activity;

- The provider's procedures for ensuring its foreign resellers maintain an appropriate CIP;

- Contact information for the person responsible for managing the CIP;

- The number and locations 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."

Thereafter, U.S. IaaS providers and their related foreign resellers must submit annual CIP certifications attesting the provider has:

- Reviewed its CIP in the year since its last certification;
- Incorporated relevant updates into its CIP concerning "changes in its service offerings;"
- Updated its CIP to incorporate changes in the cyber threat landscape;
- Ensured its CIP is in compliance with the regulations; and
- "Recorded the resolution of each situation in which the IaaS provider was unable to verify the identity of a customer since its last certification."

Providers are expected to update Commerce "outside of the normal reporting schedule . . . [if, for example,] a significant change in business operations or corporate structure has occurred or a material change to a CIP [including a change to the primary contact responsible for the CIP] has been implemented." The reference to a change in "corporate structure" is interesting, and raises the question as to whether Commerce might expect providers to notify Commerce of an acquisition or significant investment into the company. (Commerce may clarify this point in a final rule.)

Further, new providers of IaaS products must submit a completed CIP certification form to Commerce prior to granting IaaS account access to any foreign customer.

3. ***Compliance Assessments***

To guarantee compliance with the proposed rule, Commerce will review all information submitted by U.S. IaaS providers and their related foreign resellers in annual CIP certification forms. If a CIP fails to meet the requirements set forth above, Commerce may:

1. Conduct a compliance assessment of certain IaaS providers; or
2. Audit the "provider's CIP processes and procedures."

Following a compliance assessment or audit, Commerce may:

1. Recommend certain remediation measures; and
2. "Review a specific transaction or a class of transactions" carried out by an identified IaaS provider.

IaaS providers are expected to maintain a written copy of both their CIP and their foreign resellers' CIPs, and "must provide any copy of these CIPs to [Commerce] within ten calendar days of a request from [Commerce]."

4. ***CIP Exemptions***

An IaaS provider may apply for an exemption from the CIP requirement by demonstrating that it has established an appropriate Abuse of IaaS Products Deterrence Program ("ADP") aimed at "detect[ing], prevent[ing], and mitigat[ing] malicious cyber enabled activities."

The Secretary of Commerce considers the following, "in consultation with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence," when determining whether to issue an exemption:

1. Whether the ADP is of "an appropriate size and complexity;"
2. Whether the ADP incorporates a "robust" ability to "deter, detect, and respond to red flags;"
3. Whether the provider maintains "effective" oversight of reseller arrangements;
4. The extent to which the provider voluntarily cooperates with law enforcement; and
5. Whether the provider participates in public-private sector collaborations meant to "develop and maintain privacy-preserving data sharing and analytics to enable improved detection and mitigation of malicious cyber-enabled activities."

Once an exemption is granted, the IaaS provider and its foreign resellers must regularly update their ADP to incorporate the "changing threat landscape" and must notify the Secretary of Commerce of any "significant deviations or changes to their ADP."

Special Measures for Certain Foreign Jurisdictions or Foreign Persons

The proposed rule authorizes the Secretary of Commerce to prohibit or limit, for a period of 365 days unless extended, IaaS transactions with:

1. Certain foreign persons who have "engaged in a pattern of malicious cyber-enabled activities;" or
2. Persons located in certain foreign jurisdictions which have a "significant number of foreign persons offering . . . or directly obtaining U.S. IaaS products for use in malicious cyber-enabled activities."

If the Secretary of Commerce issues a written determination barring or limiting interactions with a certain foreign person or jurisdiction, U.S. IaaS providers must incorporate the special measures no earlier than 180 days following the determination.

Reporting Certain Large AI Model Training

In an effort to secure the development and use of artificial intelligence ("AI"), the proposed rule requires U.S. IaaS providers and their foreign resellers to report known instances of foreign persons training "large AI models with potential capabilities that could be used in malicious cyber-enabled activity" to Commerce.

If a U.S. IaaS provider becomes aware of a transaction concerning a foreign person which:

1. “Results or could result in the training of a large AI model with potential capabilities that could be used in malicious cyber-enabled activity;” or

2. “[While] the original arrangements provided for in the terms of the transaction would not result in [the aforementioned training,] 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,”

the provider must file a report with Commerce, including relevant information about the foreign person and training run, within 15 days of the “transaction occurring or the provider or reseller having knowledge” of the prohibited transaction. U.S. IaaS providers may refer to the examples provided in § 7.308 for additional information.

A U.S. provider of IaaS products may not provide products to a foreign reseller who does not comply with identified reporting requirements.

Key Takeaways

The proposed rule by Commerce reflects an effort to secure the American cyber frontier, particularly in relation to the development of artificial intelligence. The following aspects and implications of the proposed regulations are notable:

- The proposed rule would institute a CIP requirement for U.S. IaaS providers akin to the “know your customer” requirements applicable to banks, introducing a complex compliance protocol that will require resources and lead time.

- Under the proposed framework, companies can seek an exemption from the CIP requirement by adopting an ADP and applying to Commerce for an exemption.

- Under the proposed rule, U.S. companies newly seeking to become IaaS providers would need to adopt a CIP before starting business as a provider.

- The proposed rule’s reporting requirements regarding foreign persons’ use of IaaS products to engage in certain AI training would impose a significant monitoring obligation on providers.

- The proposed rule would require U.S. providers to flow the CIP and reporting requirements through to foreign resellers.

- The stakes of noncompliance would be high, with violations punishable under the International Emergency Economic Powers Act, which provides for civil penalties of up to the greater of ~$368,000 per violation or twice the value of the transaction connected to the violation, or criminal penalties of up to $1 million and/or 20 years’ imprisonment.

- Notably, Commerce is proposing to implement the rules by amending the ICTS regulations, which otherwise are focused on threats to the U.S. technology supply chain. The technology should monitor developments relating to these rules, as they likely will be an important vehicle for technology regulation in the months and years to come.

- Commerce is also considering imposing controls on the use of U.S. export-controlled advanced computing items to provide cloud services for use in training large AI models. This is an important

part of the policy conversation and should be part of the risk calculus for companies in the industry.

- Affected or interested parties may submit comments on the proposed regulations until April 29, 2024.

For more information on the proposed rule or assistance with submitting comments, contact Anthony Rapa, Rachel D. Evans, or another member of Blank Rome's International Trade group.

PROFESSIONALS

Anthony Rapa
Rachel D. Evans

SERVICES

International Trade
Economic Sanctions, Export Controls, CFIUS & Geopolitical Risk
Government Contracts

INDUSTRIES

Technology
Privacy, Security & Data Protection

AUTHORS

Anthony Rapa
Rachel D. Evans

FIND AN ATTORNEY

A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z

OFFICES

Chicago, IL
Cincinnati, OH
Dallas, TX
Fort Lauderdale, FL
Houston, TX
Los Angeles, CA
New York, NY
Orange County, CA
Philadelphia, PA
Pittsburgh, PA
Princeton, NJ
Shanghai
Tampa, FL
Washington, D.C.
Wilmington, DE

STAY CONNECTED

Register to receive insights and analyses on breaking news and trends across varying industries.

Subscribe

PARTNER SITES

ROME

R

CONNECT

- Contact us
- Twitter
- LinkedIn
- Blogs