Published on *The National Law Review* https://natlawreview.com

Cloud Services Compliance: Scrutiny on Foreign Access to U.S. Infrastructure as a Service

Article By:

Kara M. Bombach

Cyril T. Brennan

Sonali Dohale

Claudia D. Hartleben

Kyle R. Freeny

Jena M. Valdetero

On January 29, 2024, the U.S. Department of Commerce (Commerce)'s Bureau of Industry and Security issued a proposed rule (the Proposed Rule) that would require providers and foreign resellers of U.S. Infrastructure as a Service (IaaS) to take certain measures to identify customers and prevent foreign cyberattacks. Notably, the Proposed Rule would require implementation of Customer Identification Programs (CIP) with customer verification, monitoring, and reporting requirements relating to foreign users. Comments on the Proposed Rule must be submitted by ***April 29, 2024****.*

Overview

The use of cloud-hosted IT infrastructure has expanded significantly in recent years, prompting the U.S. government to address new risks and threats to national security posed through use of U.S. IaaS and artificial intelligence (AI).

The 2021 executive order (EO) on "Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities" announced that foreign malicious cyber actors have used IaaS products to "harm the United States economy through the theft of intellectual property and sensitive data and to threaten national security by targeting United States critical infrastructure for malicious cyber-enabled activities." Citing difficulty tracking and obtaining information through legal process before evidence is destroyed, the EO authorized Commerce to establish identity verification and recordkeeping obligations on U.S. providers of IaaS to bolster security and investigation efforts.

The 2023 EO on “Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence” additionally directed Commerce to require U.S. IaaS providers to report “when a foreign person transacts with that United States IaaS Provider to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity (a ‘training run’),” among other requirements.

To implement these EOs, the Proposed Rule would require U.S. providers of IaaS, including any U.S. and foreign resellers, to verify their customers and undertake monitoring and reporting requirements to protect against foreign cyber actors from using their services to engage in malicious activity.

Scope of Affected Entities

Direct providers and any U.S. resellers are considered “U.S. IaaS providers” subject to the proposed regulations. The Proposed Rule defines IaaS as “any 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 expansive proposed definition captures “all service offerings for which a consumer does not manage or control the underlying hardware,” such as content delivery networks, proxy services, and domain name resolution services.

A “foreign reseller” is proposed to mean “a foreign person who has established an IaaS Account to provide IaaS subsequently, in whole or in part, to a third party.”

Under the Proposed Rule, U.S. IaaS providers would be required to collect identifying information and verify the identity of beneficial owners of accounts owned or maintained by entities. Commerce proposes that “beneficial owner” mean “an individual who either: (1) exercises substantial control over a Customer, or (2) owns or controls at least 25 percent of the ownership interests of a Customer.”

New Customer Identification Program Requirements

A key feature of Commerce’s Proposed Rule would obligate U.S. IaaS providers and their foreign resellers to develop and maintain a risk-based Customer Identification Program (CIP). While companies would be able to tailor their CIPs to their specific business and risk profile, CIPs would have to meet certain minimum requirements, including:

- **Data Collection**. Collecting identifying information about foreign account holders and their beneficial owners, including name, address, means and source of payment for each customer’s account, email addresses and telephone numbers, and IP addresses used for access or administration of the registered account.

- **Identity Verification**. Verifying the identity of all foreign account owners and foreign beneficial owners through procedures that will “allow providers to form reasonable beliefs of the true identity of each customer and beneficial owner.” The CIP would also need to specify remedial steps, where the provider is unable to verify a customer’s identity.

- **Retention and Reporting Requirements**. Establishing procedures for collecting and maintaining verification information, and resolution of “any substantive discrepancy discovered when verifying the identifying information.” Commerce proposes a two-year record retention period after the date upon which an account was last accessed or closed.

Providers must annually update the CIP to protect against threats and certify to Commerce to completion of the update.

Commerce proposes that U.S. IaaS providers and their foreign resellers must establish a compliant CIP within one year of the date of publication of any final rule and notify Commerce that final provisions have been implemented. U.S. IaaS providers must furnish “a copy of any foreign reseller’s CIP” to Commerce “within ten calendar days” following such request.

Notably, U.S. IaaS providers and their foreign resellers may be granted an exemption from the new CIP requirements where Commerce finds the applicant complies with security best practices to otherwise deter abuse of IaaS products. Commerce invites stakeholder input on crafting the exemption criteria.

Steering Clear of Special Measures

The 2021 EO authorized Commerce to prohibit or impose conditions on a new or existing U.S. IaaS account in a foreign jurisdiction or by a foreign person (the Special Measures). The Special Measures may be taken where Commerce determines that “reasonable grounds exist 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.’”

Commerce will investigate whether available evidence provides “reasonable grounds” for imposition of either Special Measure. The Proposed Rule lists factors Commerce must consider, centering on the extent to which the U.S. IaaS product is used to conduct, facilitate, or promote malicious cyber-enabled activities.

AI Training

Pursuant to the 2023 EO, the Proposed Rule also would require reporting instances when a foreign person transacts with the U.S. IaaS provider to use the U.S. IaaS product to train a “large AI model with potential capabilities that could be used in malicious cyber-enabled activity,” defined as:

any AI model with the technical conditions of a dual-use foundation model, or that 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, as necessary and appropriate of cyber operations.

Reportable information would include the customer’s identifying information and the existence of the training run.

Enforcement

Non-compliance with IaaS or AI-related requirements in any final rule would be subject to civil penalties of up to the greater of $250,000 per violation or twice the amount of the transaction value, and criminal penalties of up to $1,000,000 per willful violation or up to 20 years’ imprisonment, or

both.

Key Takeaways

If your company may be covered by the new compliance regime, consider participating in the rulemaking process by submitting comments on the Proposed Rule. Key ambiguities include:

1) The scope of who is covered by the compliance obligations, which stem from the proposed definition of “U.S. IaaS product,” stated above;

2) How “substantial control” over a customer should be interpreted, in the definition of “beneficial owner”; moreover, whether the 25% threshold in the proposed definition is appropriate and feasible for purposes of the proposed regulations;

3) Whether there exist security best practices to deter abuse of U.S. IaaS products that can be referenced in future authorization of CIP exemptions;

4) Challenges U.S. IaaS providers would face in investigating and remediating malicious cyber activity by foreign resellers, and any commercial implications posed by terminating the relationship for non-compliance;

5) The definition of “large AI model with potential capabilities that could be used in malicious cyber-enabled activity.”

Comments must be received by April 29, 2024.

Given the short implementation period envisioned by the Proposed Rule, companies that may be subject to the CIP requirements should consider assessing their current methods of collecting customer information.

David A. Zetoony contributed to this article.

National Law Review, Volume XIV, Number 71