Alert

February 27, 2024

U.S. Department of Commerce Proposes a New KYC Rule Applicable to U.S. IaaS Providers

On January 29, 2024, the U.S. Department of Commerce's (Department) Bureau of Industry and Security issued a notice of proposed rulemaking (Proposed Rule) that proposes a new Customer Identification Program (CIP) and other requirements applicable to U.S. providers and foreign resellers of infrastructure as a service (IaaS) products.

Definition of IaaS Product

The Proposed Rule defines an IaaS product 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." Further, the Proposed Rule clarifies that a "consumer typically does not manage or control most of the underlying hardware but has control over the operating systems, storage, and any deployed applications." An IaaS product 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 that the product is available to the consumer."

Applicability of the CIP Requirements

The Proposed Rule would require U.S. IaaS providers and their foreign resellers to verify the identity of their foreign customers and report to the Department on the use of their products for large artificial intelligence training.

If the Proposed Rule is approved in its current form, it would mandate that a U.S. IaaS provider working with a foreign reseller must ensure that the foreign reseller maintains and implements a written CIP as specified by the Proposed Rule and submit the foreign reseller's CIP to the Department within 10 calendar days of a request.

Overview of the CIP Requirements

The Proposed Rule requires each U.S. IaaS provider of IaaS products to maintain and implement a written CIP. A U.S. reseller may adopt its direct provider's CIP to comply with the Proposed Rule.

Additionally, a U.S. IaaS provider must ensure that foreign resellers of U.S. IaaS products maintain and implement a written CIP. The U.S. IaaS provider must provide the foreign reseller's CIPs to the Department within 10 calendar days of the Department's request. The CIP must include risk-based procedures used to verify the identity of each foreign customer that enable the U.S. IaaS provider or foreign reseller of U.S. IaaS products to form a reasonable belief that it knows the true identity of each customer.

The CIP must contain procedures that enable the U.S. IaaS provider or foreign reseller of U.S. IaaS products to determine whether a potential customer and all beneficial owners are U.S. persons. Furthermore, CIP must contain procedures for opening an IaaS account that specify the identifying information that will be obtained from each potential customer and beneficial owners of the customer that will be used to determine whether they are U.S. persons.

All U.S. IaaS providers and all of their foreign resellers of U.S. IaaS products must obtain, at a minimum, the following information from potential foreign customers or foreign beneficial owners prior to opening an account: (i) name, (ii) address, (iii) means and source of payment for the IaaS account, (iv) email address, (v) telephone number, and (vi) IP addresses. The collected data must then be verified through documentary and/or non-documentary methods. For an IaaS provider that

Robert W. Rubenstein

Associate

rrubenstein@cozen.com
Phone: (215) 366-4472
Fax: (215) 665-2013

Christopher Dodson

Member

cdodson@cozen.com
Phone: (215) 665-2174
Fax: (215) 372-2408

Related Practice Areas

- Business
- Corporate
- Technology, Privacy & Data Security

relies on documentary methods, the CIP must contain procedures that set forth the documents the IaaS provider will use and its method for ascertaining the documents are valid. With respect to an IaaS provider relying on non-documentary methods, the CIP must contain procedures that describe the non-documentary methods the IaaS provider will use.

The CIP must include procedures for responding to circumstances in which the U.S. IaaS provider or foreign reseller of U.S. IaaS products cannot form a reasonable belief that it knows the identity of a customer or beneficial owner. These procedures should address when the U.S. IaaS provider should (i) not open an IaaS account, (ii) grant a temporary and restricted account while the IaaS provider attempts to verify the identity of a customer or beneficial owner of the account, (iii) close the IaaS account or impose additional monitoring on the relevant account, or (iv) take other measures for IaaS account management or redress for customers who could not be verified or whose information may have been compromised.

Exemptions from CIP Requirements

U.S. IaaS providers may seek an exemption from the CIP requirements. The Secretary of Commerce (Secretary) may grant an exemption if it determines that the U.S. IaaS provider complies with security best practices to deter the abuse of IaaS products and has established an Abuse of IaaS Products Deterrence Program (ADP). The Proposed Rule includes a list of requirements that a U.S. IaaS provider's ADP must meet to qualify for an exemption from CIP requirements

To determine whether a U.S. IaaS provider qualifies for an exemption from the CIP requirements, the Secretary will make a finding based on an evaluation of certain factors, such as (i) whether the ADP is an appropriate size and complexity commensurate with the nature and scope of product offerings; (ii) the ADP's ability to deter, detect and respond appropriately to any red flags that have been identified; (iii) whether the U.S. IaaS provider has implemented appropriate and effective oversight of reseller arrangements with respect to detecting and mitigating red flags; (v) the extent of voluntary cooperation with law enforcement, consistent with otherwise applicable law, to provide forensic information for investigations of identified malicious cyber-enabled activities; and (vi) the participation in government collaboration efforts. In the Proposed Rule, the Department defines red flags as "a pattern, practice, or specific activity that indicates the possible existence of malicious cyberenabled activities."

U.S. IaaS providers would have a continuing obligation to update their ADPs regularly in response to the changing threat landscape and would be required to notify the Secretary of any significant deviations or changes to their ADPs. All U.S. IaaS providers must provide information on such updates by submitting annual notifications for themselves or any of their exempt foreign resellers to the Department to ensure that exemptions from the CIP requirements continue to be granted.

CIP Certification and Reporting

Each U.S. IaaS provider must notify the Department of the implementation of its CIP and, if relevant, the CIPs of each foreign reseller of its U.S. IaaS products, through the submission of a CIP certification form.

U.S. IaaS providers must submit to the Department certifications of their CIPs on an annual basis and, if relevant, the CIP of each foreign reseller of its U.S. IaaS products. The annual certifications may be submitted to the Department at any time within one year of a previous submission, but no earlier than 60 calendar days prior to that date.

Each U.S. IaaS provider must notify the Department if, outside of the normal reporting schedule outlined in the Proposed Rule, a significant change in business operations or corporate structure has occurred or a material change to a CIP has been implemented, to include, for example, a material change in the documentary or non-documentary methods of identity verification or in the procedures for handling unverified accounts.

Prior to furnishing any foreign customer with an IaaS account, any newly established U.S. IaaS provider must notify the Department of the implementation of their CIP through submission of their CIP certification form.

Reporting of Large AI Model Training

The Proposed Rule requires U.S. IaaS providers to report transactions by, for, or on behalf of a foreign person, involving the training of a large AI model that could be used in malicious cyber-enabled activities (each, a Covered Transaction). U.S. IaaS providers are required to file a report with the Department within 15 calendar days of a Covered Transaction occurring, or the provider or reseller having "knowledge" that a Covered Transaction has occurred. In the Proposed Rule, the Department defines knowledge as "[k]nowledge of a circumstance (the term may be a variant, such as "know," "reason to know," or "reason to believe")," 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."

U.S. IaaS providers must also require their foreign resellers to file a report with the U.S. IaaS provider 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 is required to file this report with the Department within 30 calendar days of the Covered Transaction. In its current form, the Proposed Rule does not explicitly address what the U.S. IaaS provider is required to do if it is notified by its foreign reseller months later.

Compliance Assessments

All U.S. IaaS providers of U.S. IaaS products must maintain copies of the CIPs of any of their foreign resellers. Additionally, all U.S. IaaS providers must provide a copy of any of these CIPs to the Department within 10 calendar days of a request from the Department.

If the Department finds that a CIP from either a U.S. IaaS provider or their foreign reseller fails to meet the certification and reporting requirements of the Proposed Rule, then the Department will notify the relevant IaaS provider of the deficiencies identified in the CIP. If the Department notifies an IaaS provider of any deficiencies, the IaaS provider would be required to resolve the identified deficiencies within a reasonable time period, as determined by the Department, and to resubmit the CIP for further inspection.

Additionally, the Department has the sole discretion (as to time and manner) to conduct compliance assessments of U.S. IaaS providers based on the Department's own evaluation of risks associated with a given CIP, the U.S. IaaS provider, or any of its foreign resellers.

The Department has the sole discretion to evaluate risks based on its own criteria, which includes (i) assessing whether the services or products of a U.S. IaaS provider or a foreign reseller are being used or are likely to be used by foreign malicious cyber-actors, or by a foreign person to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity; or (ii) the failure of any U.S. IaaS provider of IaaS products to submit a CIP certification or implement measures recommended by the Department as the result of a compliance assessment.

Based on the results of a compliance assessment, the Department may take action, such as: (i) recommending that remediation measures be taken by the U.S. IaaS provider to address any risk of U.S. IaaS products being used in support of malicious cyber activity or to train a foreign-owned large AI model with potential capabilities that could be used in malicious cyber-enabled activity; or (ii) reviewing a transaction or class of transactions of an IaaS provider.

Enforcement and Penalties

Under the Proposed Rule, it is a violation for any U.S. IaaS provider to fail to implement or maintain a CIP, or continue to transact with a foreign reseller that fails to implement or maintain a CIP. Violations of the requirements in the Proposed Rule are subject to civil and criminal penalties under the International Emergency Economic Powers Act. Maximum civil penalties are $250,000 per violation (subject to inflationary adjustment), or an amount that is twice the amount of the transaction that is the basis of the violation, whichever is higher. Criminal penalties for willful actions range up to $1 million in fines, up to 20 years in prison, or both.

Conclusion

If the Proposed Rule is approved in its current form, U.S. IaaS providers will have compliance obligations with respect to their transactions with foreign customers. U.S. IaaS providers will also need to put in place procedures that are designed to hold their foreign resellers accountable for

CIP maintenance reporting rules, along with satisfying reporting requirements for large AI model transactions. Industry members can submit comments on various aspects of the Proposed Rule, which must be received by April 29, 2024. Given the increased compliance costs and risks for U.S. IaaS providers, such providers and their resellers should begin planning their CIPs.