Commerce Proposes KYC and Other Cybersecurity Requirements on Cloud Services and AI Training

Eric McClafferty, Wyatt Mince

February 6, 2024

On January 29, 2024, the Commerce Department's Bureau of Industry and Security (BIS) published a notice of proposed rulemaking (NPRM) introducing a Customer Identification Program (CIP) and other requirements applicable to U.S. providers and foreign resellers of Infrastructure as a Service (IaaS) products. The proposal also includes reporting requirements covering foreign transactions with U.S. cloud services to train "dual-use" AI foundational models that may enable malicious cyber activity. The NPRM implements Executive Orders addressing threats to U.S. critical infrastructure or national security posed by malicious, cyber-enabled activities.

The Commerce Department is soliciting comment on the proposed rules for 90 days, with submissions due to the agency by April 29, 2024. Key features of the NPRM and areas for comment are summarized below.

Customer Identification Program

The new rule would require that U.S. providers of IaaS products (including U.S. resellers) implement and maintain a written, risked-based Customer Identification Program (CIP). The CIP is a Know-Your-Customer (KYC) program that would consist of data collection procedures for ascertaining and verifying the identities of current and prospective customers. Importantly, the requirement extends to confirming beneficial owners. For many companies, the requirements extend beyond the identification information currently collected from customers. Moreover, U.S. IaaS providers would need to ensure that foreign resellers of their IaaS products maintain and implement adequate CIP programs. U.S. IaaS provider would need to terminate their relationship with foreign resellers who do not adequately comply. To reduce compliance burdens, the Department proposes to allow foreign resellers, by agreement, to adopt or reference CIP programs created by U.S. IaaS providers. Providers would need to report to Commerce that they and their foreign resellers have a CIP, and annually certify information about the CIP thereafter. Although the Department is considering an adjustment period, compliance with any final rule would be required within one year of publication.

In response to comment, the Department has clarified that foreign subsidiaries of U.S. IaaS providers would not be covered under the current interpretation of the rules.

Additionally, the NPRM envisions a mechanism for requesting exemption from CIP requirements, and requests comment on proposed standards and procedures for adjudicating the same. The Department also welcomes information regarding (1) security best practices to deter abuse of U.S. IaaS products and (2) safe harbor activities that may form the basis of an exemption.

Special Measures

The NPRM proposes a procedure for imposing restrictions on certain foreign persons opening or maintaining IaaS accounts. Notably, the Department would be empowered to impose restrictions on specific foreign actors and all customers and potential customers within a specified foreign jurisdiction. If the Department exercises this authority, companies would need procedures in place to make sure prohibited foreign parties cannot open or maintain accounts. The Department would undergo a thorough investigation, based on its own accord or upon referral from other executive agencies or providers, to determine whether the following reasonable grounds exist that warrant special intervention:

- For foreign actors, the Department would need to find reasonable grounds that the person has established a pattern of conduct of offering U.S. IaaS products that are used for malicious cyber-enabled activities or directly obtaining U.S. IaaS products for use in malicious cyber-enabled activities; and
- For foreign jurisdictions, the Department would need to find a significant number of foreign persons offering U.S. IaaS products that are, in turn, used for malicious cyber-enabled activities, or a significant number of foreign persons directly obtaining U.S. IaaS products and using them in malicious cyber-enabled activities.

AI Training

In accordance with Executive Order, the proposed rule would require reports to the Department on instances of "training runs" by foreign persons for "large AI models with the potential for malicious cyber-enabled activity." The requirement would cover transactions that result **or could result** in AI training meeting certain technical conditions. Providers would need to build in procedures to identify potential transactions for reporting.

By way of example, the Department notes that a foreign corporation proposing to train a large AI model on the computing infrastructure of a U.S. IaaS provider—and signs an agreement to provide such training—would be covered by the proposed requirement so long as the AI model's specifications meet certain technical conditions. At this point, the Department's standard for determining what technical conditions trigger the AI reporting requirement would reference interpretive rules published in the Federal Register and be updated based on technological advancements.

Nonetheless, the Department seeks comment on (1) the definition of "large AI models with the potential for malicious cyber-enabled activity" and (2) what red flags the Department should adopt that would create a presumption that a foreign person is training an AI model meeting the requisite technical conditions.

Outlined in the NPRM are several other elements of and considerations relating to the proposal, including data collection requirements and a discussion of cost burdens associated with implementing a CIP program. And the Department is soliciting comment on several other areas of the rule, including challenges that U.S. IaaS providers may face in investigating and remediating malicious cyber activity, the potential impact of the rule on small businesses, and more. Again, any such comments must be received by the Department by April 29, 2024.