Simpson Thacher

# Memorandum

## BIS Publishes Proposed Rule Imposing "Know Your Customer" and Reporting Requirements on U.S. Infrastructure as a Service Providers

March 5, 2024

On January 29, 2024, the U.S. Department of Commerce's Bureau of Industry and Security ("BIS") issued a proposed rule that would impose, for the first time, detailed know-your-customer ("KYC") requirements on U.S. Infrastructure as a Service ("IaaS") providers and their foreign resellers (the "Proposed Rule"). The Proposed Rule would also allow BIS to impose "special measures" to prohibit or condition the provision of U.S. IaaS products to foreign jurisdictions and persons of concern, and require IaaS providers to report certain transactions implicating large AI models that could be used for malicious cyber-enabled activities.

The Proposed Rule comes at a time of increasing U.S. regulatory scrutiny on cloud computing and AI applications, including President Biden's landmark Executive Order directing new rulemaking on AI across federal agencies as well as BIS's latest effort to prevent China and twenty plus other countries from acquiring advanced semiconductors necessary for training large AI models. Specifically, the Proposed Rule seeks to implement (i) Executive Order 13984, which called for new regulations to prevent cyber-attacks, and certain provisions of (ii) Executive Order 14110, designed to strengthen U.S. defenses against dangerous uses of AI.

### Scope of the Proposed Rule

The Proposed Rule adopts the Executive Order 13984 definition for IaaS product, which is defined broadly to include "any product or service offered to a consumer that provides processing, storage, networks, or other fundamental computing resources and with which the customer can deploy and run software that is not predefined, including operating systems and applications."

Under this definition, the providers of various internet infrastructure services—*e.g.*, content delivery networks, proxy services and domain name resolution services—along with traditional cloud services providers would be considered IaaS providers. In contrast, domain name registration services would not fall under the definition because they do not provide any processing, storage, network, or other fundamental computing resources to the consumer.

Since the Proposed Rule applies to all U.S. IaaS providers and their foreign resellers, companies providing large-scale cloud services, internet infrastructure services, large-scale AI-focused compute services, or other services at risk for being considered IaaS should carefully review the Proposed Rule and consider submitting comments prior to the comment deadline on April 29, 2024.

## Customer Identification Program

Under the Proposed Rule, all U.S. IaaS providers must verify the identity of foreign persons that sign up for or maintain accounts that access or utilize their services. Such providers, as well as their foreign resellers, are therefore required to implement and maintain a so-called "Customer Identification Program" ("CIP") to collect certain identifying information about their customers.

The CIP must contain, among other things, procedures that would enable the U.S. IaaS provider to determine whether a potential customer and all beneficial owners are U.S. persons. If the procedures reveal that such is the case, no further tracking is required. However, for potential foreign customers or beneficial owners, the CIP must include their name, address, means and source of payment, email address, telephone number, and IP addresses, which must then be verified through documentary and/or non-documentary methods as specified in the Proposed Rule.

U.S. IaaS providers and their foreign resellers must submit to the BIS an initial CIP certification and subsequent annual certifications, notifying BIS of any updates to their CIPs or those of their foreign resellers and attesting to compliance with the regulations. A full list of requirements for CIP certifications is included in Section 7.304 of the Proposed Rule.

Compliance with the CIP requirements would be required within one year after a final rule is published, though BIS is considering allowing an adjustment period to implement at least some of the CIP requirements.

## Commerce May Impose "Special Measures" Against Specific Countries or Customers

The Proposed Rule authorizes the BIS to, under certain circumstances, impose two types of "special measures" to prevent U.S. IaaS providers from aiding malicious cyber-enabled activities. One special measure is jurisdiction-based, in which the BIS may prohibit or impose conditions on the opening or maintaining of an account with any U.S. IaaS provider or their reseller by any foreign person located in a foreign jurisdiction found to have any significant number of foreign persons offering U.S. IaaS products used for malicious cyber-enabled activities, or by any U.S. IaaS provider of U.S. IaaS products for or on behalf of a foreign person. The second special measure is individual-based, in which the BIS may prohibit or impose conditions on the opening or maintaining of an account with any U.S. IaaS provider or their reseller for or on behalf of a foreign person, if such an account involves any foreign person found to be directly obtaining or engaged in a pattern of conduct of obtaining U.S. IaaS products for use in malicious cyber-enabled activities or offering U.S. IaaS products used in malicious cyber-enabled activities. Although China is not specifically mentioned in the Proposed Rule, China and/or Chinese companies will likely be the target for the jurisdiction-based special measure.

## New Reporting Requirements for Large AI Model Training

The Proposed Rule requires U.S. IaaS providers and their foreign resellers to report to BIS any transaction with a foreign person that, based on U.S. IaaS provider's "knowledge" (including "reason to know" and "reason to

believe"), either (i) could result in the training of "a large AI model with potential capabilities that could be used in malicious cyber-enabled activity" or (ii) where a change in scope in existing uses of U.S. IaaS products results in the training of "a large AI model with potential capabilities that could be used in malicious cyber-enabled activity."

Notably, the term "large AI model with potential capabilities that could be used in malicious cyber-enabled activity" under the Proposed Rule means "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," such as social engineering attacks, data poisoning, and remote command-and-control of cyber operations. Because the "dual-use foundation model" is broadly defined under Executive Order 14110, BIS will separately specify the technical specifications for the AI models that are subject to the reporting requirements through future rulemaking and continue to update the definition as the technology continues to evolve.

The reports to the BIS must include the identity of the foreign person and the existence of any training run of an AI model. They will be due within 15 days of a covered transaction occurring or the provider or reseller having "knowledge" that a covered transaction has occurred.

## Penalties and Enforcement

Violations of the Proposed Rule could result in civil or criminal penalties imposed by the International Emergency Economic Powers Act ("IEEPA"), depending largely on the nature of the offense. Violations include both intentional and unintentional failure to create, maintain, or report a CIP, or failure to inform BIS about an IaaS transaction that might result in a customer obtaining or using a "large AI model with potential capabilities that could be used in malicious cyber-enabled activity."

As such, U.S. IaaS providers and their foreign resellers should be prepared to set up policies and procedures to ensure strict compliance once the final rule is issued.

For further information regarding this memorandum, please contact one of the following authors:

NEW YORK CITY

**George S. Wang**
+1-212-455-2228
gwang@stblaw.com

**David H. Caldwell**
+1-212-455-2612
dcaldwell@stblaw.com

**Daniel S. Levien**
+1-212-455-7092
daniel.levien@stblaw.com

BEIJING

**Yang Wang**
+86-10-5965-2976
yang.wang@stblaw.com

**Shuhao Fan**
+86-10-5965-2987
shuhao.fan@stblaw.com

PALO ALTO

**Bo Bryan Jin**
+1-650-251-5068
bryan.jin@stblaw.com

WASHINGTON, D.C.

**Abram J. Ellis**
+1-202-636-5579
aellis@stblaw.com

HONG KONG

**Wendy Shidi Wu**
+852-2514-3488
wendy.wu@stblaw.com