ALERT MEMORANDUM

Proposed Rulemaking by U.S. Department of Commerce Introduces New Obligations on U.S. IaaS Providers and Foreign Resellers to Curb Malicious Cyber-Enabled Activities

February 7, 2024

Background:

On January 29, 2024, the U.S. Department of Commerce ("Commerce") published a notice of proposed rulemaking (the "Notice") seeking comments on proposed rules promulgated by Commerce's Bureau of Industry and Security ("BIS") and newly-created Office of Information and Communications Technology and Services to implement Executive Order 14110, the Biden Administration's October 2023 executive order on artificial intelligence ("AI") ("E.O. 14110", see our prior alert here)[1]. The Notice also implements Executive Order 13984, a 2021 executive order relating to malicious cyber-enabled activities ("E.O. 13984") (with respect to which Commerce had already issued an advanced notice of proposed rulemaking)[2].

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors

NEW YORK

Lindsay Harris
+1 212 225 2151
lharris@cgsh.com

Daniel Ilan
+1 212 225 2415
dilan@cgsh.com

Chase D. Kaniecki
+1 202 974 1792
ckaniecki@cgsh.com

Yulia Solomakhina
+1 212 225 2848
ysolomakhina@cgsh.com

[1] Exec. Order. No. 14110, 88 Fed. Reg. 75191 (Nov. 1, 2023).
[2] Exec. Order No. 13984, 86 Fed. Reg. 6837 (Jan. 25, 2021).

Both executive orders include provisions directing the Secretary of Commerce (the "Secretary") to propose regulations obligating U.S. infrastructure as a service ("IaaS") providers and their foreign resellers to collect, verify, maintain, and report to the Secretary certain information pertaining to foreign customers, including relating to foreign customers' use of U.S. IaaS products to train large AI models for purpose of carrying out malicious cyber-enabled activities. We provide below further detail on the meaning under the Notice of "U.S. IaaS Providers", "foreign resellers" and "IaaS products".

The proposed rules are part of efforts by the Administration to mitigate the risk of foreign malicious cyber actors using U.S. IaaS products to commit intellectual property and sensitive data theft, to engage in covert espionage activities, and to threaten national security by targeting U.S. critical infrastructure. Foreign malicious cyber activities targeting the United States have been a point of concern for various departments and agencies within the executive branch, such as the National Security Agency[3] and the U.S. Department of the Treasury, which recently imposed sanctions on actors responsible for engaging in such activities.[4] The Notice highlights the difficulty of preventing and addressing such vulnerabilities without the ability to identify specific malicious foreign actors, which the proposed requirements of the rules would endeavor to do. If implemented, violations of the rules could result in civil or criminal penalties. Comments to the proposed rules are due to BIS by April 29, 2024.

The Notice:

Identification and Verification of Customers by Customer Identification Programs: The proposed rules set forth in the Notice would require U.S. IaaS providers and their foreign resellers to implement customer identification programs ("CIPs"), similar to the Know Your Customer procedures required under anti-money laundering and counter terrorism financing regulations and also used for sanctions compliance purposes. The Notice sets forth the minimum requirements for what should be included in the CIP (including personal information regarding foreign customers such as their name, address, email, telephone number, credit card number and IP address), but notes that any CIP must be "risk-based", i.e., appropriate for the IaaS provider's size, products offered, and customer base. Under the proposed rules, U.S. IaaS providers are required to:

- maintain a written CIP;
- ensure foreign resellers implement and maintain a CIP;
- provide copies of their and their foreign resellers' written CIP upon the Secretary's request;
- notify Commerce of implementation of their and their foreign resellers' CIP through a certification form, and annually attest that the CIP has been reviewed to account for any changes in the service offering and the threat landscape;
- submit ad hoc reports to Commerce on the occurrence of certain changes/updates to the provider's company, services, threat landscape, or the CIP between annual certifications;
- report on certain AI-related transactions (see more detail on reporting on large AI model training below); and
- maintain records related to the Notice for at least two years from the date an IaaS account was closed or last accessed.

If a U.S. IaaS provider finds that a foreign reseller has failed to maintain a CIP or has demonstrated lack of good faith efforts to prevent the use of U.S. IaaS products for malicious cyber-enabled activities, the IaaS provider must take steps to close the foreign reseller's account and report any suspected or actual

[3] Russian Cyber Actors are Exploiting a Known Vulnerability with Worldwide Impact > National Security Agency/Central Security Service > Press Release View (nsa.gov)

[4] Treasury Sanctions Actors Responsible for Malicious Cyber Activities on Critical Infrastructure | U.S. Department of the Treasury

malicious cyber-enabled activity to the relevant authorities. U.S. IaaS providers are further required to terminate relationships with any foreign reseller within 30 calendar days if the U.S. IaaS provider has actual or constructive knowledge that the foreign reseller has not remediated issues identified by such provider, or if the continuation of the provider/reseller relationship augments the risk of the U.S. IaaS products being used for malicious cyber-related activity.

Reporting Training of Large AI Models with Potential Capability for Malicious Cyber-Enabled Activity: The proposed rules also would require U.S. IaaS providers to submit reports to Commerce when they have knowledge of "a transaction by, for, or on behalf of a foreign person which results or could result in the training of a large AI model with potential capabilities that could be used to enable malicious cyber-enabled activity". Notably, the term "large AI model with potential capabilities that could be used in cyber-enabled activity" under the Notice 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, vulnerability discovery, denial-of-service attacks, data poisoning, target selection and prioritization, misinformation generation and/or propagation, and remote command-and-control of cyber operations. Because the definition of "dual-use foundation model" (DUFM")[5], which is consistent with the definition under E.O. 14110, is new and written broadly, it is difficult to determine with any certainty whether particular models will or will not qualify as a DUFM. Moreover, the Secretary is instructed to specify the technical conditions for large AI models to have the said potential capabilities and to revise the determination as necessary, so the scope will evolve. Given the adaptability of many large-scale computing models, though, it is possible that this definition would capture more than might be obvious, such as text-to-image generators (which, for example, could pose a risk to national security if a user generated a violent or political image that is used to disseminate misinformation).

Special Measures for Certain Foreign Jurisdictions and Foreign Persons: Under E.O. 13984, the Secretary also may require U.S. IaaS providers to prohibit or limit access to accounts used by particular foreign malicious cyber actors if, after consultation with the appropriate federal agencies, the Secretary finds reasonable grounds to conclude that a foreign jurisdiction has a significant number of foreign malicious cyber actors using U.S. IaaS products, or a foreign person has established a pattern of conduct of offering U.S. IaaS products that are used for malicious cyber-enabled activities. The Notice does not suggest any specific foreign jurisdictions be covered at this time.

Exemptions: U.S. IaaS providers may seek an exemption from the CIP requirements, and Commerce may grant exemptions upon a determination that a 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 Notice sets forth numerous fairly stringent requirements for the ADP, including regular updates, employee training, annual certifications and oversight

[5] E.O. 14110 defines a "dual-use foundation model" generally to include any AI model that: (i) is trained on broad data, (ii) generally uses self-supervision, (iii) contains at least tens of billions of parameters, (iv) is applicable across a wide range of contexts and (v) exhibits, or could be easily modified to exhibit, high levels of performance at tasks that pose a serious risk to security, national economic security, national public health or safety or any combination thereof. Models meet this definition even if they are provided to end users with technical safeguards that attempt to prevent users from taking advantage of the relevant unsafe capabilities. It further enumerates examples of such risks, including:

(i) substantially lowering the barrier of entry for non-experts to design, synthesize, acquire, or use chemical, biological, radiological, or nuclear (CBRN) weapons;

(ii) enabling powerful offensive cyber operations through automated vulnerability discovery and exploitation against a wide range of potential targets of cyberattacks; or

(iii) permitting the evasion of human control or oversight through means of deception or obfuscation.

infrastructure. Such requirements potentially could make establishing an ADP more burdensome than simply complying with the CIP requirements. The Notice also seeks comments regarding the criteria Commerce can use to exempt U.S. IaaS providers or specific types of accounts from the reporting requirements.

Proposed Definitions of U.S. IaaS Provider, Foreign Reseller, and IaaS Product: U.S. IaaS provider is defined in the Notice to mean any U.S. person that offers a product or service 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. Commerce proposes to adopt the definition of "foreign reseller" from E.O. 14110, meaning any foreign person who has established a U.S. IaaS account to provide IaaS to a third party. An account established by a U.S. person could qualify as a foreign reseller account if the beneficiary is a foreign person. The definition of "IaaS Product" would capture content delivery networks, proxy services, and domain name resolution services, but not domain name registration services because the third party does not provide any processing, storage, network, or other fundamental computing resources to the consumer in such instances. Examples of some of the largest IaaS providers include Digital Ocean, Verizon, IBM, Microsoft, Google, VMWare and Citrix.

Potential Conflict with Data Privacy Law: At first glance, the required disclosure of personal information regarding customers and foreign cyber actors seems to run afoul of data privacy laws abroad, such as the EU General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act ("CCPA"). However, because there are exceptions under the applicable regulations for disclosure of personal information (for example where disclosure is required to comply with law), the proposed rule might not necessarily conflict with a company's obligations thereunder. It remains to be seen whether these required disclosures would fit squarely within one of those exceptions, and Commerce is seeking comments on the impact any proposed regulations would have on data protection and security, especially considering the GDPR and the CCPA.

Key Takeaways:

— While the proposed rules will inevitably result in increased costs for U.S. IaaS providers, there may be ways for companies to build upon existing compliance practices. For example, screening and verification of customers could likely be undertaken using the same screening tools as companies may use for various other compliance efforts, including sanctions compliance purposes (e.g., the databases which provide information on the corporate tree, sanctions and other notable red flags). The resulting risk analysis could go in parallel with anti-money laundering and sanctions compliance assessments.

— In addition to those specific areas mentioned above, Commerce is seeking comments from industry participants on existing best practices. Because the proposed rules only establish the minimum parameters, a risk-based approach is suggested, such that providers should assess their specific customer base and products and understand the relevant risks to which they are exposed to take appropriate mitigation measures. The comment period presents an opportunity for members of the private sector to provide input on the risks specific to their businesses, highlight the practical considerations of creating a potentially significant new compliance regime, and offer ways to build in efficiencies and ensure operational feasibility.

…

CLEARY GOTTLIEB