INSIGHT | March 14, 2024

Proposed Regulations for U.S. IaaS Providers: Enhancing Cybersecurity for Cloud Services and AI Training

Executive Summary

In response to evolving cybersecurity threats in the digital landscape, the U.S. Department of Commerce (the "Department") has proposed comprehensive regulations aimed at fortifying cybersecurity measures for U.S. Infrastructure as a Service (IaaS) providers and their foreign resellers. These proposed regulations, outlined in the Proposed Rule issued on January 29, 2024 (available here), introduce stringent Customer Identification Program (CIP) requirements and reporting obligations pertaining to the training of large artificial intelligence (AI) models with potential capabilities for malicious cyber-enabled activities. This article summarizes the key provisions of the Proposed Rule and their implications for industry stakeholders, providing a comprehensive analysis of the regulatory landscape and its impact on the IaaS sector.

Background

The Proposed Rule stems from mounting concerns over national security risks associated with the use of IaaS products, particularly in the context of malicious cyber-enabled activities. Executive orders issued in 2021 and 2023 highlighted the increasing threat posed by foreign actors exploiting vulnerabilities in U.S.

cloud computing infrastructure to steal sensitive data and intellectual property, engage in covert espionage activities, and launch disruptive cyberattacks targeting critical industries.[i] These concerns underscored the need for regulatory measures to enhance the identification and monitoring of foreign users of IaaS products, as well as to establish mechanisms for reporting and mitigating potential risks associated with large AI model training. Consequently, the Department issued the Proposed Rule to impose detailed CIP, or know-your-customer (KYC), requirements on U.S. IaaS providers and their foreign resellers[ii], aimed at bolstering cybersecurity efforts and safeguarding national interests against evolving cyber threats.

Definition and Scope of IaaS Products

Central to the Proposed Rule is the definition and scope of IaaS products[iii], which encompasses a broad spectrum of services providing fundamental computing resources to consumers. These services include processing, storage, and network capabilities, catering to the diverse needs of businesses and individuals in the digital ecosystem. Moreover, the definition of IaaS products extends beyond traditional offerings to include managed and unmanaged services, virtualized and dedicated products, as well as auxiliary services such as content delivery networks, proxy services, and domain name resolution services. This expansive definition underscores the regulatory intent to encompass a wide array of IaaS offerings under the purview of the Proposed Rule, ensuring comprehensive coverage and oversight in the realm of cybersecurity.

CIP Requirements

A cornerstone of the Proposed Rule is the establishment of robust CIPs[iv] by U.S. IaaS providers and their foreign resellers, aimed at verifying the identity of foreign customers and beneficial owners[v], mitigating risks associated with malicious cyber activity, and ensuring compliance with regulatory standards. These CIPs are envisaged as comprehensive frameworks encompassing various elements, including customer identification, identity verification, record retention, and security protocols. Specifically, U.S. IaaS providers are mandated to develop and maintain written CIPs, while also ensuring that their foreign resellers adhere to similar standards. Key components of these CIPs include:

- **Customer Identification**: The collection of comprehensive identifying information from potential foreign account holders and their beneficial owners, encompassing names, addresses, the means and source of payment for each customer's account, email addresses, telephone numbers, and IP addresses used for access or administration of registered accounts.

- **Identity Verification**: Implementation of risk-based procedures to verify the identity of all foreign customers and their beneficial owners, with documentation of verification methods and protocols for addressing discrepancies or unverified identities. If a U.S. IaaS provider or their foreign reseller cannot form a reasonable belief that it knows the identity of a customer or beneficial owner, they must implement specific remedial measures outlined in their CIP, including refraining from opening an IaaS account, granting a temporary and restricted account pending identity verification, closing the account or imposing additional monitoring, or taking other appropriate actions to manage the account or provide redress for customers who could not be verified or whose information may have been compromised.

- **Record Retention and Security**: Establishment of robust procedures for securely storing and maintaining verification records for a minimum period of two years after an account is closed or last accessed, along with protocols for addressing data breaches or unauthorized access. Providers must also annually update the CIP to protect against threats and certify to the Department to completion of the update.

Notably, U.S. IaaS providers and their foreign resellers may be granted an exemption from these new CIP requirements if they are able to demonstrate that they have implemented security best practices that adequately identify, detect, and respond to red flags via establishing an Abuse of IaaS Products Deterrence Program (ADP).[vi]

Reporting Requirements for Large AI Model Training

As noted in the background section of the Proposed Rule, the "emergence of large-scale computing infrastructure—to which U.S. IaaS providers and foreign resellers provide access as a service, and which foreign malicious actors could use to train large AI models that can assist or automate their malicious cyber activity—has raised considerable concern about the identities of entities that transact with providers to engage in certain AI training runs."

To address this and similar concerns, the Proposed Rule imposes reporting requirements on U.S. IaaS providers pertaining to transactions involving the training of large AI models with potential capabilities for malicious cyber-enabled activities.[vii] Specifically, U.S. IaaS providers are obligated to file a report with the Department within 15 calendar days of a "covered transaction"[viii] occurring, or upon obtaining "knowledge"[ix] that such a transaction has taken place. Covered transactions encompass those conducted by, for, or on behalf of foreign individuals or entities and entail the training of AI models with specific technical parameters indicative of their potential for facilitating malicious cyber activities.

Moreover, U.S. IaaS providers are required to ensure that their foreign resellers also submit reports within the same timeframe following a covered transaction. These reports must be forwarded to the Department within 30 calendar days of the transaction's occurrence. The reporting framework underscores the importance of timely and comprehensive information sharing to enable effective monitoring and response to potential cybersecurity threats arising from the training of AI models. By facilitating the identification and assessment of AI-related risks, these reporting requirements contribute to bolstering national security measures and safeguarding against the misuse of advanced technologies for malicious purposes.

Compliance Assessments and Enforcement

The Proposed Rule empowers the Department to conduct compliance assessments of U.S. IaaS providers and their foreign resellers, evaluating risks associated with CIP implementation and adherence. Non-compliance with CIP requirements may result in civil and criminal penalties under the International Emergency Economic Powers Act, highlighting the imperative of robust compliance measures and proactive risk mitigation strategies. In particular, 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 that is the basis of the violation, and criminal penalties of up to $1,000,000 per willful violation or up to 20 years' imprisonment, or both. Furthermore, the Department retains discretion

to review transactions or classes of transactions, assess compliance risks, and recommend remediation measures to ensure regulatory compliance and cybersecurity resilience within the IaaS sector.

Next Steps

The Proposed Rule represents an aggressive regulatory push to more broadly oversee the cybersecurity of U.S. IaaS providers and their foreign resellers, ushering in enhanced CIP requirements and reporting obligations to fortify cyber defenses and safeguard critical digital infrastructure. Industry stakeholders are encouraged to provide comments on the Proposed Rule before the **April 29, 2024** deadline, thereby contributing to the formulation of a robust regulatory framework that balances cybersecurity imperatives with industry innovation and growth. As the digital landscape continues to evolve, proactive engagement with regulatory authorities and diligent compliance with cybersecurity standards will be paramount for ensuring resilience and sustainability in the dynamic IaaS ecosystem.

If you have any questions about this article, please contact:

Robert McHale, Esq.
R | McHale Law
9 West Broadway, Suite 422
Boston, MA 02127
Tel. 617.306.2183
Email: robert.mchale@rmchale.com

---

[i] See Executive Order 13894 ("Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber- Enabled Activities") and Executive Order 14110 ("Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence").

[ii] The Proposed Rule adopts the E.O. 14110 definition of "foreign reseller" to mean a foreign person who has established an IaaS Account to provide IaaS products subsequently, in whole or in part, to a third party. In turn, an IaaS account is defined under E.O. 13984 to mean a "formal business relationship established to provide IaaS products to a person in which details of such transactions are recorded."

[iii] The Proposed Rule adopts the E.O. 13984 definition of "Information as a Service Product," which is "any product or service 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 consumer typically does not manage or control most of the underlying hardware but has control over the operating systems, storage, and any deployed applications." The Department seeks comment on the categories of products or services that fall within this definition.

[iv] Under the Proposed Rule (§ 7.301), "Customer Identification Program or CIP" is defined as "a program created by a United States IaaS provider of U.S. IaaS products that dictates how the provider will collect identifying information about its customers, how the provider will verify the identity of its foreign customers, store and maintain identifying information, and notify its customers about the disclosure of identifying information."

[v] Under the Proposed Rule (§ 7.301), "beneficial owner" is defined as "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." The Department seeks comments on this proposed definition, including the meaning of "substantial control."

[vi] See § 7.306 of the Proposed Rule for further details regarding CIP exemptions.

[vii] Under the Proposed Rule (§ 7.301), "large AI model with potential capabilities that could be used in malicious cyber-enabled activity" is 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." The Department seeks comment on this proposed definition.

[viii] "Covered transactions" are defined as any transactions by, for, or on behalf of a foreign person (i) "which results or could result in the training of a large AI model with potential capabilities that could be used in malicious cyber-enabled activity"; or (ii) "in which the original arrangements provided for in the terms of the transaction would not result in a training of a large AI model with potential capabilities that could be used in malicious cyber-enabled activity, but a development or update in the arrangements means the transaction now does or could result in the training of a large AI model with potential capabilities that could be used in malicious cyber-enabled activity." Proposed Rule (§ 7.308(b))

[ix] The Proposed Rule adopts the Export Administration Regulations' definition of "knowledge," which is "knowledge of a circumstance … including 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. Such awareness is inferred from evidence of the conscious disregard of facts known to a person and is also inferred from a person's willful avoidance of facts." 15 CFR 772.1.