April 29, 2024

Kellen Moriarty
U.S. Department of Commerce
Docket Number: 240119-0020
Document Number: 2024-01580
IaaScomments@bis.doc.gov

Re: Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities
(*Docket No. 240119-0020*)

The Cloud Service Providers-Advisory Board (CSP-AB) welcomes the opportunity to respond to the Department of Commerce (the "Department") Notice of Proposed Rulemaking ("NPRM" or the "Proposal") that follows the Executive Order "Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities." While we share the U.S. Government's goal of advancing national security objectives, including deterring foreign malicious cyber actors, we have concerns that the Proposal may prove ineffective in satisfying stated objectives, conflict with essential data privacy and security principles that underpin American technological leadership, and face practical and workability challenges.

The CSP-AB represents the world's leading cloud companies and supports standards and policies that promote and enable secure cloud adoption in the public and private sectors. Our member companies are global leaders in the drive to provide safe, scalable, and accredited digital government services, with a focus on both the civil servants delivering those services and the end-users receiving them. Collectively, our members hold over 700 authorizations to operate (ATOs) across all service models and impact levels, and adhere to U.S. Government FedRAMP requirements, which in a number of instances are inconsistent or incompatible with the NPRM.

While the CSP-AB supports the overarching rationale of the Proposal, we are concerned that the impact on IaaS providers is significant without demonstrating the commensurate benefits that the new requirements would bring about.

In summary:

- The CSP-AB is concerned that imposing overbroad, prescriptive bank-like Know Your Customer (KYC) requirements, as put forward in the Proposal, is impractical and burdensome, and is unlikely to enhance national security or cyber defenses. In particular, we urge reconsideration of overbroad identity verification requirements that will prove unworkable and detract resources from more effective measures to combat malicious actors.

- The CSP-AB considers the proposed definition of foreign ownership to be unduly broad. As a minimum, we encourage alignment with the Office of Foreign Assets Control (OFAC) standards.
- The CSP-AB urges the Department to focus on the development of requirements related to Abuse of IaaS Products Deterrence Programs (ADPs) instead of an overbroad CIP Rule; additionally, whether as a standalone ADP requirement or exception from the CIP Rule, CSP-AB suggests using FedRAMP as a baseline for ADP requirements to avoid duplication or fragmentation of such standards.
- The requirements related to reporting of large AI model training present significant concerns for CSPs, as among other things, it would contradict the FedRAMP shared responsibility model and privacy standards. We urge the Department to bifurcate consideration of AI reporting to a separate process and dialogue with the private sector.

§§ 7.302-7.305 Comments on the Customer Identification Program (CIP) Regulations

A. *Imposing Bank-Like KYC and Identity Verification Requirements at Scale is Overbroad, Unworkable and Would Undermine U.S. Technological Leadership.*

Imposing blanket global bank-like KYC requirements on IaaS products, particularly for small and medium-sized CSPs, is overbroad, unworkable, and an inefficient approach to deterring abuse. While the CSP-AB supports the policy intention of requiring minimum standards for IaaS providers, certain aspects of the draft requirements regarding KYC and identity verification raise significant concerns.

More specifically, blanket imposition of KYC requirements will prove overly burdensome with little clear benefit in satisfying government objectives. While specific, targeted, and defined KYC requirements in certain scenarios may be appropriate, the current Proposal fails to set forth when such requirements would be high-value. Instead, the current overbroad KYC mandates will likely prove unworkable and distract resources focused on developing more effective solutions, including those based on security best practices.

Additionally, the stringent identity verification procedures mandated for foreign customers are particularly concerning as they could exacerbate privacy concerns and strain resources, especially for CSPs with significant foreign customer bases, thereby undermining the competitiveness of U.S. companies in global markets. As noted above, this focus on new extensive verification compliance measures will divert attention and resources away from implementing robust security practices that are more effective in mitigating cyber risks.

CSPs already adhere to numerous best practices to mitigate cyber risks, including those requirements that derive from FedRAMP. Rather than imposing additional compliance burdens and obligations on CSPs with uncertain benefits for national security or cyber defenses, we advocate for a narrowly tailored targeted KYC approach. This targeted approach would delineate specific scenarios and objectives for each KYC process, allowing CSPs to implement additional measures as needed to ensure bad actors are not accessing critical services. Such an approach would not impose KYC and identity verification requirements, especially where the risk level is low.

Additionally, we advocate for a concerted effort to ensure that all CSPs meet a high security standard, including those promulgated by FedRAMP or NIST. By exploring, developing, and prioritizing the adoption of cybersecurity best practices, the Government can better safeguard against potential security threats and promote innovation in the cloud computing sector.

The lack of clarity in the proposed CIP requirements, coupled with the added complexity of managing additional record-keeping and identity verification requirements, presents a significant challenge for CSPs. Verifying identities, for instance, is not consistent with business practices for establishing a relationship with an IT service provider and certainly extends beyond CSPs' usual responsibilities; as such, it would pose a substantial burden as CSPs will be required to stand up entirely new compliance teams to develop and implement identity verification processes. Financial institutions have entire departments devoted to KYC and expend significant resources on their programs. CSPs will have to divert resources away from proven (and developing) security practices to address these new compliance requirements, without clear benefit.

Compliance with the proposed rule would further entail cumbersome reporting mechanisms, which would place a heavy burden on infrastructure providers without clear understanding of how such information will be used. This includes the need for detailed documentation of foreign customers, potentially encompassing all resellers, and a thorough documentation of the CIP. Compliance would also require comprehensive reporting on the number and types of customers, addressing any anomalies that may arise, and promptly responding to requests from the Department, which would divert provider resources from more effective approaches to addressing malicious activity.

In light of these challenges, and as detailed further below, the CSP-AB proposes prioritizing the development and adoption of cybersecurity standards and best practices as the primary approach to safeguard against security threats and promote innovation in the cloud computing sector.

B. Foreign beneficial owner requirement is unduly burdensome and broad

Further, we are concerned that the requirement to verify the identity of all customers' foreign beneficial owners will be particularly burdensome for CSPs, without effectively mitigating malicious cyber activity. CSP customers likely will have difficulty complying with foreign beneficial owner requirements, as determining foreign beneficial ownership can be a complex process that requires access to extensive corporate documentation. Verifying the identity of each foreign beneficial owner will require significant time and resources by CSPs. At the same time, malicious actors will be able to easily evade the requirement by simply stating that they do not have any foreign beneficial owners when opening an account.

Moreover, the definitions of foreign beneficial ownership are extremely broad. Specifically, under the current definition, a firm would be considered to have foreign ownership if owned or controlled by a non-U.S. person with at least 25 percent of the ownership interests. This poses a potential issue for entities with a small group of founders, predominantly U.S. citizens and all U.S. based, where even one non-US citizen among them could classify the whole company as foreign. The requirement is also likely to present considerable challenges and raise concerns for customers.

As such, we advocate for the Department to exclude the foreign beneficial owner requirement from the rule, as it extends beyond the requirements of Executive Order 13984. If the Department keeps the requirement, it should adopt a more precise definition of foreign ownership that aligns with targeted approaches as noted above. For example, if a company has one foreign owner but three U.S. owners, the risk of hostile foreign activity is significantly lower. Thus, adopting a more nuanced approach to defining foreign ownership can better accommodate risk-based considerations and reduce unnecessary burdens on entities primarily owned and operated within the United States.

To address this, at the very least, there should be alignment with standards set by the Office of Foreign Assets Control (OFAC). According to OFAC, entities are considered blocked if they are owned 50 percent or more (directly or indirectly) in the aggregate by one or more blocked persons.

C. *Request for Extension of Adjustment Period for Implementation of CIP Regulations for U.S. IaaS Providers*

The CSP-AB notes that the Department is considering allowing U.S. IaaS providers an adjustment period of one year from publication date of any final rule to implement some provisions of this proposed regulation. We recommend extending this period to at least two years, as providers will need significant time to put in place compliant programs. We also recommend this adjustment period be extended to all proposed provisions relating to CIP regulations given the time needed for proper implementation.

§§ 7.306 Comments on Exemption Regulations

As a threshold matter, CSP-AB believes that the Government will better satisfy its security objectives by focusing on establishing security standards that apply to the industry rather than an overbroad and onerous KYC mandate that will likely prove unworkable and ineffective. Instead, as discussed below, an ADP requirement is a more effective way to combat bad actors and malicious use. While such an ADP requirement is preferred, in the event that the Proposal maintains a KYC requirement, the CSP-AB generally supports the CIP exemptions outlined in §§ 7.306. However, we seek certain clarifications on the proposal that an IaaS provider could be exempted from the CIP requirements in §§ 7.302 and 7.304 if they have established an ADP.

As currently proposed, the incentives for CSPs to adopt the ADP remains unclear given its non-defined parameters and requirements. The discretionary nature of the exemption and the absence of due process in challenging revocations create uncertainty for providers. Instead, the parameters of an ADP should be clearly established in order to incentivize adoption of an ADP.

To this end, the CSP-AB urges the Department to reference and rely on FedRAMP standards as a baseline for ADP requirements. FedRAMP presents a strong foundation in defining such requirements and can avoid unnecessary duplication, conflict, or confusion regarding parallel standards. Beyond FedRAMP, we believe there are additional security best practices that can help underpin ADP requirements. We provide such additional best practices for consideration here, but urge the Department to develop these standards further in partnership with the private sector:

1) Establish and enforce terms of service that clearly prohibit malicious cyber activity and detail actions to be taken in response to activity found to be in violation of those terms.

2) Provide means and instructions for third parties to easily report suspected or confirmed abuse and monitor and act on such reports in a timely manner.

3) Maintain a compliance program and establish policies and practices for addressing government requests for data associated with law enforcement investigations, in accordance with relevant data privacy requirements.

4) Implement account creation and resource allocation processes to mitigate the risk of fraud.

5) Document, maintain, and implement internal policies and procedures for detecting, mitigating, and responding to abuse, including by:

a. Establishing steps to identify and evaluate accounts suspected of conducting malicious activity, fraud or abuse;

b. Implementing steps to mitigate the offending behavior such as via restricting account access to new resources, requiring further proof of legitimacy, and/or removing resources engaged in malicious activity; and

c. Establishing metrics for reducing abuse and continually measuring performance against them.

6) Prohibit the use of payment instruments for IaaS services that can increase anonymity.

§§7.308 Reporting of large AI model training

CSP-AB respectfully recommends that the Department bifurcate consideration of the proposal regarding reporting of large AI model training to a separate process given a number of challenges with the proposed rule. Such consideration should allow for constructive public-private dialogue in order to satisfy governmental interests, while addressing industry concerns.

More specifically, the CSP-AB acknowledges the definition in §§7.308 (B)(2), stipulating that "A model shall be considered to be a large AI model with potential capabilities that could be used in malicious cyber-enabled activity". However, we seek further clarification regarding this definition and the potential for redefining technical thresholds. As currently drafted, the AI definitions are ambiguous and the requirements are in conflict with key standards and best practices. We recommend, for example, that the Department engage with industry to develop specific and narrow technical criteria for the types of models that should be subject to discussion. Such criteria may include compute capacity and type of infrastructure used to train the model, which are the only criteria into which a provider normally has visibility.

Additionally, the proposed AI reporting requirements present significant concerns for CSPs. It would require CSPs to report on customer AI training practices and cybersecurity procedures, directly contradicting the shared responsibility model. The requirement presupposes that CSPs will have visibility into customer models trained on their infrastructure and engage in ongoing monitoring, which is not feasible. For example, triggering the reporting requirement based on customer activity indicating potential malicious cyber-enabled activity implies that CSPs possess insights into customer activity and the capabilities of these models. Additionally, the requirement includes reporting instances of insider threat events where unauthorized access to customer models may have occurred. The requirements contradict the core principle of the Customer Responsibility Matrix outlined in FedRAMP's Appendix J, which aims to prevent CSPs from accessing customer workloads.

Given these challenges, CSP-AB suggests that the AI reporting requirements be subject to further discussion and collaboration with the industry. While we share the goal of deterring and preventing malicious activity, the current proposal raises significant challenges and concerns that outweigh any perceived benefits.

* * *

We thank you for your consideration of our comments on this important topic and would welcome serving as a resource in consideration of this Proposal. As noted above, we strongly urge continued consideration of existing challenges within the Proposal to ensure the development of efficient and effective solutions.

Sincerely,

LNava

Laura Navaratnam

Executive Director

The Cloud Service Providers - Advisory Board

lnavaratnam@csp-ab.com

http://csp-ab.com