Subject*:* Comments on "E.O. 13984/E.O. 14110: NPRM."

To Whom it May Concern:

On behalf of The Digital Chamber ("the Chamber"), we respectfully submit our comments on the U.S. Bureau of Information Security's (BIS) notice of proposed rulemaking requiring U.S. Infrastructure as a Service (IaaS) providers of IaaS products to verify the identity of their foreign customers.

The Chamber is the world's first and largest blockchain trade association. Our mission is to promote the acceptance and use of digital assets and blockchain technology. We are supported by a diverse membership that represents the blockchain industry globally. Through education, advocacy, and close coordination with policymakers, regulatory agencies, and industry across various jurisdictions, our goal is to develop a responsible, pro-growth environment for digital assets highlighting all the opportunities this emerging industry will present to the United States. Our members include the industry's leading innovators, operators, advisory firms, and investors in the blockchain ecosystem.

The Chamber acknowledges the well-intentioned essence of the recent regulatory proposal. However, we must express our profound reservations about the potentially expansive implications of the rule's broad language, particularly as it pertains to distributed ledger and blockchain technologies due to the decentralized nature of these systems.

It's crucial to strike a balance between addressing national security concerns and preserving the innovative potential and core values of distributed ledger technologies. Engaging with industry stakeholders, technology experts, and international partners will be essential in crafting practical and effective compliance measures that can be implemented without stifling the growth and adoption of these technologies.

Challenges

The proposed rule poses significant compliance challenges for decentralized IaaS providers, which are exacerbated by the unique nature of a decentralized environment. The rule's requirements for customer interaction and the gathering of Know Your Customer (KYC) information may not be feasible for decentralized IaaS providers, who may lack direct customer relationships.

Even when such a relationship does exist, these often-small-scale providers do not possess the resources of traditional IaaS entities to meet the demands to comply with the rule.

Moreover, the proposed definition of an IaaS product, which is "any product or service offered 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" is not applicable to most of the decentralized, blockchain-based products in existence, which can be cloud solutions but not specifically cloud-computing solutions, since they do not allow the deployment of non-predefined software by the consumer.

Additionally, virtual machines (VMs) on blockchain networks, while capable of running smart contracts, are not designed to support complex or continuously operational software due to inherent constraints such as gas fees, transaction speeds, and memory limits. These blockchain VMs, serving primarily to enable blockchain functionality, do not pose the same risk level as traditional cloud computing products and thus should be considered outside the rule's intended scope.

This illustrates how the rule, as written, could exclude blockchain protocols that offer specialized infrastructure services outside of the computing spectrum, suggesting that the rule may not be appropriate or intended for such blockchain protocols.

Recommendations

To ensure regulatory measures are effectively tailored and applicable, we recommend the explicit exclusion of blockchain-based IaaS and decentralized, permissionless products that are not offering cloud-computing solutions from the scope of the proposed rule.

The definition of an IaaS product, which is contingent on the ability to deploy and run non-predefined software, does not align with the fundamental nature and technical operations of many blockchain protocols, which offer infrastructure services but not in the traditional sense of cloud computing.

Additionally, as BIS continues to adapt to a rapidly evolving digital and decentralized economy, traditional approaches like KYC protocols require re-examination to ensure they remain effective without encroaching on individual privacy. To navigate this transition successfully, it is imperative for BIS to engage with industry leaders, particularly those in the distributed ledger technology sector, to collaboratively devise solutions that uphold safety while respecting the decentralization ethos and privacy needs of users.

The first step in this collaborative process should involve identifying and integrating technological solutions that do not compromise on privacy yet offer robust verification and monitoring capabilities. For instance:

1. Collaborate with DLT Providers and Experts:
    a. Forge partnerships with DLT experts to conceptualize and develop identity verification systems that are inherently privacy-preserving. By tapping into the expertise of those at the cutting edge of blockchain technology, BIS can explore innovative approaches that align with decentralized models.

b. Engage in joint development initiatives to create transaction monitoring tools that respect user anonymity while still providing the necessary oversight required by regulatory bodies.

2. Leverage Emerging Cryptographic Technologies:
    a. Investigate the integration of zero-knowledge proofs (ZKPs) within the compliance frameworks. ZKPs allow for the verification of transactions or identities without revealing underlying data, thus maintaining user privacy.
    b. Evaluate the potential of secure multi-party computation (SMPC), which could enable the processing of encrypted data by multiple parties without exposing the actual information to any single entity, thereby preserving confidentiality.
    c. Explore other advanced cryptographic methods that can be tailored to maintain the integrity of transactions and identity checks in a manner that is both secure and private.

The goal of these initiatives would be to strike a balance between regulatory compliance and the preservation of the privacy and autonomy that are hallmarks of decentralized systems. Through continuous dialogue and pilot projects, BIS and DLT providers can set a precedent for regulatory innovation that could be emulated globally. It's about creating a framework that is not just compliant but also conducive to the trust and freedom that underpin the digital, decentralized economy. This forward-thinking approach could result in a compliance landscape that is adaptable, secure, and, most importantly, respectful of individual privacy.

We appreciate the opportunity to provide comments on this important topic. The Chamber and its membership hope to serve as a resource to BIS as comments are considered and look forward to further engagement.

Sincerely,

Cody Carbone

Cody Carbone
Chief Policy Officer