W3WG **WEB3 WORKING GROUP**

Apr 29, 2024

Alan F. Estevez
Under Secretary of Commerce for Industry and Security
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, DC 20230
IaaScomments@bis.doc.gov

**Re: Department of Commerce; Request for Comment (E.O. 13984/E.O. 14110: NPRM)**

To Whom It May Concern:

Web3 Working Group is a leading nonprofit organization in the decentralized technology space. It educates and champions the growth and advancement of decentralized physical infrastructure networks (DePIN) and the broader web3 ecosystem. Web3 Working Group seeks to position the United States at the forefront of emerging web3 technologies.

Web3 Working Group shares the government's aim of preventing foreign actors from exploiting domestic cloud computing resources for malicious cyber activities. However, we are concerned that as currently written, the rule is significantly overbroad and could have unintended consequences for the growing American DePIN sector. The plain language of the definition of IaaS Product potentially includes not only the main cloud computing resource providers, which may be attractive targets for malicious actors, but also most of the projects in the DePIN space which not only are of no threat to American cybersecurity broadly. However the projects would find it nearly impossible to comply with the requirements as written.

As such, Web3 Working Group believes that the rule should be changed to exempt DePIN protocols and similarly situated services from the proposed Commerce Rules "Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities."

## I. Background on DePIN

The DePIN sector offers an alternative to centrally controlled internet and related technology infrastructure. DePIN protocols allow companies or individuals to purchase these services in a decentralized manner, as opposed to purchasing exclusively from large companies like Microsoft or Amazon Web Services. There are many competing protocols in the sector, some examples include: the Akash network, which facilitates cloud computing rentals, the Filecoin and Arweave networks, which facilitate decentralized data storage, both metered and permanent, Helium, which enables the purchase of internet service, and IoTex, which enables cryptographically secure geolocation tracking for logistics and a number of other use-cases.

Beyond the technological impact of their decentralized nature, these networks are also different from current web analogs because purchasing the service doesn't depend on credit cards or traditional payment rails. The functionality, security, and economics of these services revolve around the network's native token and how its issuance is designed before release. For instance, the Arweave network for decentralized persistent storage uses the Arweave token, or AR. The users who provide the storage on the network get paid in those AR tokens, but to give them incentive to provide the service before there were many users of it (the boot-strapping problem), the protocol provides a subsidy in the form of newly created tokens, which reduces over time as adoption grows.

There are multiple reasons for building systems around these tokens. For instance, the token structure allows users to pay for and receive services without a middleman or payment processor. Without a native token, a centralized middleman would be necessary, negating the decentralized network's purpose. Native tokens also incentivize individuals to participate in and grow the network during a project's startup phase.

All of these factors serve to make the DePIN sector significantly different from traditional web services for which this rulemaking was written.

## II. The Definition of “Infrastructure as a Service Product” is Overly Broad

As proposed, the definition of IaaS Product likely includes a broad swath of technologies that do not function as cloud services providers, cannot be effectively used to train adverse AI models, or otherwise pose a threat of being susceptible to foreign exploitation for malicious cyber activity.  One reason that the definition of IaaS Product is susceptible to over expansive interpretation lies, in part, with the use of vague terms like “predefined” software and “proxy services.”  These terms can easily be constructed to include the services that DePIN protocols offer even though there is no one entity that is in control of providing those services.

It is currently unclear how the Department will interpret the term “predefined” software, which could be particularly problematic for the many DePIN protocols which run under “predefined” conditions such as how information is stored, or data processed.  Similarly, “proxy services” could refer to a wide range of software tools and applications, including practically any network components that serve as intermediaries for routing information between users and DePIN protocols.  Without further clarity and refinement with these terms the definition of IaaS Product could inappropriately capture most of the DePIN sector.

To illustrate the overbreadth of the definition the following are examples of DePIN protocols which would likely be caught up in current definitions. The current definition reads “processing, storage, network, or other fundamental computing resources with which [a] consumer is able to deploy and run software that is not predefined,”

For processing that could capture protocols like Akash which provides general processing power for a variety of use-cases or Render which provides computing power specifically for video encoding and AI training.

For storage it could capture protocols like FileCoin which allow for metered decentralized file storage or Arweave which allows for permanent decentralized file storage.

While all of these protocols are growing and providing significant value for American consumers and consumers across the world, none of these protocols represent a significant threat to American national cybersecurity.

There are a number of ways decentralized networks can explicitly ensure that they cannot be used for sophisticated cyberattacks. Decentralized networks are not “botnets” in which some remote user is able to exert a great deal of control of a batch of other people’s computers, without their permission or awareness. Rather, decentralized networks are inhospitable to this type of activity because they run with the *permission* of the people that own the computers the protocol runs on, and they are in absolute control of how their hardware is used. For example, storage networks like FileCoin and Arweave give their service providers the ability to decide what information they store.

Processing networks work in one of two ways. First, there’s specialized processing which asks a group of nodes to all run the same software with some type of coordination between them to produce a specific type of output - like video renders, chatbot responses and math calculations. Specialized processing networks cannot be used by foreign actors to run malicious programing because of their specific nature.

These networks are designed to run code that comes from specific channels and utilize strong cryptography to ensure they aren't tricked. Second, there's general processing, which takes the form of markets that let developers rent virtual machines to run any kind of code, from websites to chatbots to app store games. These would be an appealing vector for a foreign actor, except they can be shut off by their owners if they detect that they're being used for malicious cyber attacks or other illegal activity.

As the Department evaluates next steps in implementing the Proposed Rule, we would encourage it to be explicit that DePIN protocols are specifically excluded from these definitions.

## III. Other Blockchain Technologies

A potentially expansive interpretation of IaaS Product could also capture blockchain technologies which underpin the nascent web3 ecosystem but do not qualify specifically as DePIN.  One example are smart contracts which are open-source software tools that can be user-specified, and users can deploy and interact with them on decentralized blockchains that users do not themselves host.  The Proposed Rule does not mention smart contracts or other blockchain-related technologies, suggesting they are not intended to be captured by this rule.

Additionally, the Department indicates that there must be a "formal business relationship" between an IaaS Product provider and user, in order for the Proposed Rule to apply. This likely means that decentralized blockchain protocols could not fall within the proposed rules because no formal business relationship exists between blockchain protocols and users.  If this is the case, the Department should specify that the proposed rules do not apply.

## IV. Acquiring Regulatory Certainty Can Be Too Onerous and Expensive

It should be noted that the Proposed Rule provides potential relief for these providers through its risk-based approach to Customer Identification Programs (CIP), as well as standards and procedures for securing exemptions from CIP requirements.  However, these pathways are not optimal with regards to U.S. innovation in the DePIN and blockchain space.  Obtaining regulatory certainty still requires companies or protocols to expend significant legal resources in determining whether the Proposed Rule applies to them.  If the Proposed Rule applies, the company or protocol would then have to expend additional resources to enact policies and procedures implementing the rules or to apply to the Department for relief.  Due to this vagueness, thousands of potential companies or projects could fall within the scope of the Proposed Rule, which would lead to a tremendous waste of resources and slow American innovation in the DePIN and blockchain space.

A better regulatory path forward would be to add clarifying language exempting DePIN protocols and blockchain protocols explicitly. Given the nature of these projects, the ability for them to be used by malicious foreign actors is essentially zero.

## V. The Proposed Rule May Move DePIN Offshore

The lack of clarity around the regulations of tokens which underpin DePIN projects has already led to many of them moving offshore. These projects and protocols are the building blocks of the new internet and such projects moving offshore harms American competitiveness. If there is a lack of clarity in Proposed rule, America will once again continue to push more of these projects offshore.

This would have the dual purpose of not only forgoing the economic benefits of such innovation, but if DePIN presents any risk at all, it would all but  remove the ability for American law enforcement to have any power to intervene.

## VI. Conclusion

Web3 Working Group appreciates the opportunity to comment on the Proposed Rule. While we share the Department's concerns regarding the cyber threats posed by malicious foreign actors, we urge the Department to focus their time on the actors in this space which are large enough targets for malicious foreign governments while providing the clarity and needed exemption for DePIN and blockchain to continue to develop in the United States.