Consumer Technology Association™

1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

April 29, 2024

Kellen Moriarty
Bureau of Industry and Security
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, DC 20230

(via Regulations.gov)

Re: E.O. 13984/E.O. 14110: NPRM – Docket No. DOC-2021-0007

Mr. Moriarty,

Consumer Technology Association (CTA)®[1] appreciates the opportunity to comment on the Department of Commerce (Department) Bureau of Industry and Security (BIS) *Notice of Proposed Rulemaking* (*NPRM*) on proposed rules to require U.S. Infrastructure as a Service (IaaS) providers to verify the identity of their foreign customers, along with procedures for the Secretary to grant exemptions and special measures to deter foreign malicious cyber actors' use of U.S. IaaS products.[2] We share the Administration's commitment to securing U.S. infrastructure and persons against foreign malicious threat actors. Indeed, many of CTA's more than 1300 members are providing and/or leveraging IaaS products and AI applications to bring innovative technologies to consumers around the world.[3] Consumer trust is vital to this effort. That's why CTA and its members have been strong partners to the U.S. government and are working every day to bring enhanced security innovations to the information and communications technology and services (ICTS) ecosystem to the benefit of consumers.

[1] As North America's largest technology trade association, CTA® is the tech sector. Our members are the world's leading innovators—from startups to global brands—helping support more than 18 million American jobs. CTA owns and produces CES®—the most powerful tech event in the world.

[2] *Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities*, 89 Fed. Reg. 5698 (Jan. 29, 2024) (*NPRM*).

[3] For example, CTA dedicated an entire category of Innovation Awards to those products demonstrating excellence and innovation in AI at CES 2024, recognizing 37 different products and services just in this category alone. CTA, CES 2024 Innovation Awards, https://www.ces.tech/innovation-awards/honorees.aspx (last visited Apr. 26, 2024); *see also* CTA, CES® 2024 Innovation Awards Product Categories, https://www.ces.tech/innovation-awards/categories.aspx (last visited Apr. 26, 2024).

CTA recognizes the Department's work to meet the goals and directives set forth under Section 4.2(c) of EO 14110 on "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" and the earlier EO 13984 on "Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities."[4] However, CTA is concerned that the proposed rules take an overbroad approach in attempting to tackle disparate issues under a single regime that will undermine the government's ultimate goals and result in the over regulation of emerging technologies.

Over-regulation stifles innovation and job growth. As CTA CEO Gary Shapiro has previously testified, "the cost of over-regulation [for small businesses and startups] means the difference between survival and failure" and "[u]nnecessary mandates not only waste taxpayer money – they impose burdens that slow innovation, stifle creativity, reduce consumers' choices and ultimately threaten jobs and the economy."[5] This is truer today than ever before. Particularly given the nascency of the technologies implicated under the proposed rules, the Department should significantly tailor the scope of these requirements.

In general, a more targeted rule will support the Department's implementation of the rule. Among other changes to more precisely tailor the scope of the rules, the definition of "IaaS product" should exclude products like blockchain, as well as content delivery networks (CDNs), proxy services, and domain name resolution services (i.e., DNS resolution) which do not provide the same threat vector that the rules are designed to address. In addition to requiring U.S. IaaS providers and resellers to implement CIPs to support the Departments' efforts to identify and address foreign malicious use of U.S. IaaS infrastructure, the *NPRM* proposes rules to require providers of certain IaaS products to report to the Secretary when a foreign person transacts with that provider or reseller to train a large artificial intelligence (AI) model with potential capabilities that could be used in malicious cyber-enabled activity. AI is an emerging technology, with complex challenges that are distinct from those raised in relation to CIPs for other types of services. As drafted, the *NPRM* risks conflicts of law and may undermine international coordination efforts to establish common standards and tools for AI risk management. Unlike other aspects of the *NPRM*, the AI training requirements are so novel that they require additional expert and multi-stakeholder collaboration on any potential proposed rules, let alone final rules.

As discussed below, CTA urges the Department to tailor its rules more narrowly to address specific IaaS products and separate its treatment of AI training reporting requirements to allow for necessary stakeholder input.

---

[4] Exec. Order No. 14110, 88 Fed. Reg. 75191 (Oct. 30, 2023) (EO 14110); Exec. Order No. 13984, 86 Fed. Reg. 6837 (Jan. 19, 2021).

[5] Testimony of Gary Shapiro to Senate Commerce, Science, and Transportation Committee, at 8-9 (Feb. 1, 2017), https://www.commerce.senate.gov/services/files/b6d4fe57-528c-4f53-9ed2-f75fcee8eaf0.

I. A Narrower Scope Will Enable the Department to More Effectively Implement the Rules and Avoid Conflicts and Enforcement Challenges

Tailoring the scope of covered products will make for more effective rules and reduce compliance challenges for products and services ill-fit for the proposed requirements. The *NPRM* intentionally proposes a broad scope, particularly with respect to "IaaS product," which it defines as "*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*."[6] This broad scope could inadvertently encompass products and services that the rules are not designed to address, and which already have controls in place to prevent their use by foreign malicious cyber actors.[7]

The proposed rules should not apply to blockchain infrastructure as either a practical or policy matter because blockchain does not have a central entity for implementing CIPs and does not face the threats the NPRM seeks to address. Under the proposed IaaS product definition, the rules could apply to blockchain networks and blockchain sequencers, which may be considered an "unmanaged" product or service "in which the provider is only responsible for ensuring that the product is available to the consumer," consistent with the *NPRM*'s definition.[8]

However, the proposed rules would be difficult if not impossible to implement with respect to blockchain. Blockchain networks are typically open-source software, like email or web browsing, that any individual can use and build upon without permission. Therefore, blockchain networks and protocols, as a distinct software product, cannot implement individual CIPs as they do not have a central entity to implement the program or collect the relevant information.

Furthermore, blockchain infrastructure does not lend itself to the type of malicious cyber activity the proposed rules aim to address. The decentralized, consensus-based nature of blockchains makes them significantly more resilient. Unlike other computing systems,

---

[6] *NPRM* at 5701 (*emphasis added*). The NPRM defines IaaS product as "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. 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 term is inclusive of 'managed' products or services, in which the provider is responsible for some aspects of system configuration or maintenance, and 'unmanaged' products or services, in which the provider is only responsible for ensuring that the product is available to the consumer. The term is also inclusive of 'virtualized' products and services, in which the computing resources of a physical machine are split between virtualized computers accessible over the internet (e.g., 'virtual private servers'), and 'dedicated' products or services in which the total computing resources of a physical machine are provided to a single person (e.g., 'baremetal' servers)."

[7] *NPRM* at 5702.

[8] *Id.*

blockchain networks can only be successfully attacked by controlling at least a majority of the validators on the network, which is prohibitively expensive and has never been done for the largest networks. Blockchain networks are not used as vectors to attack the United States and blockchain code, by design, is open and visible to anyone. Any cybersecurity threats embedded within the blockchain itself, or exploitable by malicious actors, are also visible to anyone by default. Transactions on blockchain networks with sanctioned persons are also already subject to prohibitions as with any other asset class and application provider.

Blockchain networks and sequencers are used in various consumer products and services to provide secure and transparent solutions for data management and transactions.[9] The broad scope outlined in the *NPRM* could lead to unwarranted legal challenges for blockchain businesses. This ambiguity would create a chilling effect on innovation and investment in the blockchain space, ultimately undermining the competitiveness of the United States in the global digital economy.

The proposed rules should expressly exclude CDNs, proxy services and DNS resolution. The *NPRM*'s definition of IaaS product includes criteria regarding the consumer's capabilities with respect to the IaaS product, underscoring that the consumer must be "able to deploy and run software that is not predefined," and have "control over the operating systems, storage, and any deployed applications" for the definition to apply.[10] This definition would seemingly exclude CDNs,[11] proxy services[12] and DNS resolution[13] because none of these services would

[9] *See, e.g.*, CTA, "CES 2024 Innovation Award Product: NFTCamera," (last visited Apr. 26, 2024) https://www.ces.tech/innovation-awards/honorees/2024/honorees/n/nftcamera.aspx (showcasing an app that captures and instantly secures photos in their original form on blockchain); CTA, "zkVoting: Blockchain-based voting at the Poll Station," (last visited Apr. 26, 2024), https://www.ces.tech/innovation-awards/honorees/2024/best-of/z/zkvoting-blockchain-based-voting-at-the-poll-stati.aspx (which provides the first in-person blockchain-powered voting system).

[10] *NPRM* at 5701-5702.

[11] *See* Akamai, "What Is a CDN (Content Delivery Network)?" (last visited Apr. 25, 2024) https://www.akamai.com/glossary/what-is-a-cdn (explaining that a CDN is a group of geographically distributed servers that speed up the delivery of web content by bringing it closer to where users are. Websites and web applications delivered through a CDN experience faster page loads, faster transactions, and a more consistent online experience. However, people may have no idea they are connecting through a content delivery network as they enjoy its benefits, because the technology works behind the scenes. They simply receive what they requested from their ISP or mobile provider.).

[12] *See* Palo Alto Networks, "What Is a Proxy Server?" (last visited Apr. 25, 2024) https://www.paloaltonetworks.com/cyberpedia/what-is-a-proxy-server (describing how a proxy server is a digital intermediary, routing internet traffic between users and online resources, ensuring secure and controlled data exchange. It does not provide consumers with the capability to run predefined software or give them control over operating systems, storage or deployed applications.).

[13] *See* ManageEngine, "DNS resolution: Understanding an essential part of running modern IT infrastructures," (last visited Apr. 25, 2024) https://www.manageengine.com/products/oputils/dns-resolution.html (explaining the vital role of DNS resolution in mapping human-readable domains or

allow the consumer to deploy and run non-predefined software. Nor do these services give consumers direct control over operating systems, storage or deployed applications to enable the type of malicious cyber activity the proposed rules aim to address. However, the *NPRM* later elaborates that "[t]his definition would capture services such as content delivery networks, proxy services, and domain name resolution services."[14]

The expansion of this definition countermands the focus initially established in the proposed definition, which reflects the *NPRM's* intention to address foreign malicious actors' use of U.S. IaaS products. In considering revised rules, the Department should note that CIPs cannot and should not be used to try to address every possible type of malicious cyber activity. Nor should these rules be adopted at the expense of the valuable, and in many cases vital, functions that certain types of services like CDNs, proxies and DNS resolution perform in service of global connectivity. With this in mind, the Department should revise the definition of IaaS product to explicitly exclude these types of products.

II. The Department Should Separate AI Training Reporting Requirements from the CIP Regulations

With the additional directives in EO 14110, the *NPRM* combines disparate issues in ways that would chill innovation and hinder the Administration's goals. The *NPRM* seeks to do too much and, by doing so, risks adverse consequences on the consumer technology industry. The CIP requirements envisioned in EO 13984 are not designed to address potential foreign malicious use of U.S. AI technology. Simply: not all IaaS products are AI, and not all AI is accessed as an IaaS product.

Imposing regulations on AI compute *providers* as a means of targeting AI model *developers* and *users* (the stated goal of EO 14110 and the *NPRM*) does not directly address the federal government's national security concerns regarding AI models. Instead, it creates significant bureaucratic hurdles that are unlikely to provide the information BIS is seeking and will chill innovation. U.S. IaaS providers generally do not have visibility into their customers' models, including the models' capabilities, training practices, and safeguards, all of which are critical in evaluating whether the model presents a risk. It is unlikely customers will be willing to share that information with a provider for reporting to the U.S. government (or any other purpose), given that the information is highly sensitive and proprietary. More, the inclusion of AI training reporting requirements within the CIP regulations may deter collaboration and information sharing within the AI community, hindering efforts to collectively address cybersecurity threats. Transparency and collaboration are essential pillars of effective cybersecurity strategies, and overly burdensome reporting requirements could undermine these principles.

---

hostnames with machine-readable IP addresses to enable access to websites, email servers, and other online resources).

[14] *NPRM* at 5701-5702.

Applying the proposed rules to AI products and services—especially at this early stage in the technology's development—could push companies in the AI ecosystem to foreign infrastructure providers, thereby decreasing U.S. competitiveness in AI and ultimately weakening security across the IaaS ecosystem as the U.S. cedes leadership abroad. Further, the U.S. may lose the innovation edge in AI as providers seek non-U.S. partners to avoid what may be perceived as compulsory sharing of trade secrets or other AI tradecraft under the pretext of "national security." Instead, the Department should separate its treatment of AI training run requirements into a new proceeding that allows for the stakeholder input necessary to shape the rules to effectively achieve the EO's goals.

III. The *NPRM* Risks Conflicts of Law and Undermining International Coordination Efforts

Adoption of the *NPRM* could establish a dangerous precedent justifying reciprocal efforts to require U.S. companies operating abroad to provide sensitive and proprietary information about AI model development to foreign governments. Despite discussion of privacy concerns raised in response to the *Advance Notice of Proposed Rulemaking* on EO 13984,[15] the *NPRM* does not explain which legal process it will use to compel the disclosure of AI training run data, which raises concerns regarding user privacy and customer confidentiality under laws like the Electronic Communications Privacy Act (ECPA).[16]

For example, ECPA requires the government to use a subpoena to obtain basic subscriber information (BSI), a court order for transactional information, and a warrant for content-level data.[17] Identifying information on customers' training AI models is generally classified as BSI, which includes name, address, means and source of payment.[18] In addition, the proposal regarding IP address collection may require IaaS providers to create an illegal Pen Register Trap and Trace (PRTT) as ECPA prohibits the government from requiring a provider to record or log "dialing, routing, addressing, and signaling information" without a court order mandating the creation of a PRTT.[19]

Further, the *NPRM* could foster friction with key U.S. allies and create a new target for foreign hackers. A U.S. requirement for IaaS providers to disclose sensitive foreign customer information could undermine simultaneous efforts by U.S. companies to collaborate with those in allied nations to develop common standards for AI safety and accountability across the globe. Cooperation between nations on AI safety and testing is complicated and critical to advancing democratic values in AI development, as described in the recent Memorandum of

[15] *NPRM* at 5700.

[16] 18 U.S.C. §§ 2510, *et seq*.

[17] *See* 18 U.S.C. § 2703.

[18] *See* 18 U.S.C. § 2703(c)(2)(A)-(F).

[19] *See* 18 U.S.C. § 3123.

Understanding signed between the U.S. and UK Safety Institutes.[20] Foreign governments developing AI products on trusted U.S. IaaS infrastructure may be wary to share this information in the interest of digital sovereignty.

As the Department considers revisions to the proposed rules, it should clarify how these rules will operate consistently with laws like ECPA to protect user data and support the nation's efforts to establish common approaches to safe and secure AI development and deployment with partners abroad.[21]

IV. The AI Training Requirements are Broad, Novel and Need Further Input from Stakeholders

The AI training requirements proposed in the *NPRM* are overbroad and unlikely to yield useful information about the risks that are posed by the large models on which reporting would be required. Although the initial proposals under EO 13984 have been formally studied by U.S. government representatives and industry entities, expert stakeholders have not yet afforded the *NPRM's* AI training run provisions comparable consideration.[22]

For example, compute thresholds, model capabilities and risks should inform the Department's rules regarding AI use of IaaS products. Technical criteria for a model subject to the AI reporting requirement would have to be based on the amount of compute capacity and type of infrastructure a customer uses to train a model, as these are the only criteria into which a U.S. IaaS provider will have visibility. Compute capacity, however, is only a rough approximation of the size and capabilities of a model and not a strong indicator of risk. Better benchmarks do not yet exist, however.[23] National AI Safety Institutes, including at the National Institute of Standards and Technology (NIST), are just now initiating processes to align on standard

[20] Press Release, "U.S. and UK Announce Partnership on Science of AI Safety," (Apr. 1, 2024), https://www.commerce.gov/news/press-releases/2024/04/us-and-uk-announce-partnership-science-ai-safety.

[21] The rules may also create conflicts with GDPR and the EU-US Data Privacy Framework.

[22] *See, e.g.*, NSTAC Report to the President, "Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors," (Sep. 26, 2023), https://www.cisa.gov/sites/default/files/2024-01/NSTAC_Report_to_the_President_on_Addressing_the_Abuse_of_Domestic_Infrastructure_by_Foreign_Malicious_Actors_508c.pdf.

[23] For example, AI experts recognize that Floating Point Operations Per Second (FLOPS) – a common metric currently used to measure performance and understand model risk – is not a sound indicator of risk. *See* Lark, "Flops" (Dec. 25, 2023), https://www.larksuite.com/en_us/topics/ai-glossary/flops (explaining that "[w]hile FLOPs provides a quantifiable measure of computational speed, it may not comprehensively encapsulate the intricate algorithmic complexities prevalent in advanced AI models and applications").

benchmarks for AI system and capability evaluations.[24] The "technical conditions" proposed in the *NPRM* would benefit from much more industry and stakeholder engagement before rulemaking to allow for alignment on technical benchmarks to understand large AI models that could be used for malicious activities.

By fostering an environment that encourages responsible AI development while safeguarding intellectual property rights, we can better protect critical infrastructure and advance the positive potential of AI technologies for society. To do so will require additional engagement with stakeholders before the Department adopts compliance-focused rules.

*****

CTA shares the Administration's commitment to securing U.S. infrastructure and persons against malicious cyber threats. However, proposals in the *NPRM* will hinder this effort and stifle innovation in an overbroad compliance regime. Instead, the Department should narrow the scope of IaaS products under the *NPRM* and establish a separate process for AI training requirements that solicit additional input on how to meet their unique needs. CTA welcomes further engagement with the Department on these important topics.

Respectfully submitted,

CONSUMER TECHNOLOGY ASSOCIATION

By: */s/ J. David Grossman*
J. David Grossman
Vice President, Policy & Regulatory Affairs

/s/ Doug Johnson
Doug Johnson
Vice President, Emerging Technology Policy

/s/ John Mitchell
John Mitchell
Senior Manager, Government Affairs

[24] *See* NIST, "Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence: Test, Evaluation & Red Teaming" (Jan. 26, 2024), https://www.nist.gov/artificial-intelligence/executive-order-safe-secure-and-trustworthy-artificial-intelligence/test (describing directives under EO 14110 for NIST to launch an initiative to create guidance and benchmarks for evaluating and auditing AI capabilities, develop and help ensure the availability of testing environments in coordination with the Department of Energy and National Science Foundation, and develop guidelines for AI red teaming).