Before the
U.S. DEPARTMENT OF COMMERCE
Washington, D.C. 20230

In the Matter of	)	
	)	
E.O. 13984/E.O. 14110: NPRM	)	Docket ID DOC-2021-0007
National Emergency with Respect to	)	
Significant Malicious Cyber-Enabled	)	
Activities	)	

COMMENTS OF INTERNET INFRASTRUCTURE COALITION

Christian Dawson
Ann Morton
Internet Infrastructure Coalition
2920 W Broad St. Suite 80
Richmond, VA 23230
dawson@i2coalition.com
ann@i2coalition.com

Henry Shi
HWG LLP
1919 M Street, NW, Suite 800
Washington, DC 20036
(202) 730-1348
hshi@hwglaw.com

Counsel for Internet Infrastructure Coalition

April 29, 2024

TABLE OF CONTENTS

COMMENTS OF INTERNET INFRASTRUCTURE COALITION

The Internet Infrastructure Coalition ("i2Coalition") respectfully submits comments in response to the Department of Commerce's Notice of Proposed Rulemaking, in the above-referenced docket, proposing to require United States infrastructure-as-a-service ("IaaS") providers to implement customer identification programs, among other obligations (the "Proposed Rule").[1]

I. INTRODUCTION AND SUMMARY

The i2Coalition is a global organization that supports and represents the companies that build, maintain, and operate the Internet's infrastructure. Members include cloud providers, data centers, web hosting companies, domain registries, and registrars. Our members, most of whom are small- to medium-sized businesses, but who operate globally, create a fundamental layer upon which user-facing Internet applications, services, and platforms rely and enhance that layer for security.

Promoting a secure Internet ecosystem and the responsible uses of its enabling infrastructure are core goals of the i2Coalition and its members. We appreciate the Department's publication of the NPRM and the invitation to the public to comment. As explained below, the i2Coalition has grave concerns about the Proposed Rule and its likely harmful effects on a wide range of companies in the Internet ecosystem, Internet users across the world who value the privacy and security of sensitive personal and commercial information, and ultimately the national security of the United States. The Proposed Rule suffers from a number of fatal flaws in

---

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

design and lacks any substantial support in the record as to its likely effectiveness. The most serious of these include:

- ***Overbroad Scope***. Key terms in the Proposed Rule lack coherent definitions necessary for a scope that is rationally related to the harms identified in the Executive Orders[2] prompting the NPRM and the Department's stated goals.

    - *First*, the term "infrastructure as a service product" is so vaguely defined that it can be construed to mean virtually any service provided over the Internet that allows end users to input information. This would encompass not only services that could actually be used by malicious actors to do real harm, but everyday products that most Americans who are on the Internet are likely to use regularly, like cloud storage and blogging platforms. This problem is underscored by the Department's commentary indicating that it intends to interpret the term broadly.

    - *Second*, the "minimum" requirements for mandatory "customer identification programs" ("CIP") are vastly broader and more burdensome than the NPRM recognizes and reach far beyond the required elements in the underlying Executive Order. Providers are required to verify the identity of foreign customers—and face large civil fines and potential criminal penalties if they fail to do so—but to do so accurately likely will require providers to collect and retain information from *every* customer, including every U.S. customer.

- ***No Standards for Compliance***. The unlimited scope of the Proposed Rule is made worse by the lack of any safe harbors or even clear guidance for what providers need to do, and what they do *not* need to do, in order to comply with these requirements. To verify the identity of foreign customers, providers must first be able to determine who is a foreign customer. But the global, interconnected nature of the Internet means that anyone can be a foreign customer, which in turn means that for a provider to be confident that someone is not a foreign actor, the provider must *verify* the identity of every person. The i2Coalition trusts that this is not the intended goal of the Proposed Rule. But without clear guidance that can be relied upon, responsible providers that have the resources will face overwhelming pressure to adopt conservative interpretations and overreach by default. Providers without the resources, a group consisting mostly of small and medium businesses, will have to operate under constant legal uncertainty.

- ***No Evidence of Effectiveness***. Simply put, there is zero substantial evidence in the record that the Proposed Rule will do anything to help improve U.S. national security or prevent malicious actors from using U.S. Internet infrastructure to commit crimes. It has been over three years since EO 13984 was issued on January 19, 2021, and there is no reliable data on whether and what types of IaaS products are used to commit what types of malicious cyberactivity, how much harm those activities cause, or how a CIP

[2] *See* Exec. Order 13984, 86 Fed. Reg. 6837 (Jan. 19, 2021) ("EO 13984"); Exec. Order 14110, 88 Fed. Reg. 75191 (Oct. 30, 2023) ("EO 14110" and, together with EO 13984, the "Executive Orders").

requirement would reduce those harms. To the contrary, the President's National Security Telecommunications Advisory Committee ("NSTAC") concluded the exact opposite in its recent Report to the President Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors, which is that "know your customer" ("KYC") rules described in EO 13984 are unlikely to be effective. The Department should not attempt to impose a sea change on how the Internet works based on a hunch made on the penultimate day of the last Administration.

- ***Failure to Analyze Costs***. A foundational principle of U.S. administrative law is that agencies must evaluate the potential costs and benefits of a proposed rule in order to act in a manner that is not arbitrary and capricious. The Proposed Rule failed to do this.

    - *First,* the NPRM significantly understates the burden the Proposed Rule would impose on providers of all types of services over the Internet because the actual scope of the rule is far broader than the Department suggests.

    - *Second,* the failure to adequately consider costs also stems from the enormous burden of actually complying with the CIP requirements. A 2022 survey of global banks found that KYC reviews are incredibly time consuming and costly, with banks spending anywhere from 31 to 210 days to complete a single review, at a cost of anywhere from $500 to $4500 per review.[3] This is orders of magnitude higher than Commerce's estimates of 20 minutes and $39 per CIP review and, when compounded by the broad scope of the definition of IaaS product, adds even more orders of magnitude to the total cost of implementation.

    - *Third*, the Proposed Rule does not consider at all harms its implementation would cause to the competitiveness of U.S. companies and the security of Internet users everywhere by driving users away from U.S. providers or causing them to forego services that improve their Internet security (such as proxy services).

- ***Procedural and Substantive Legal Defects***. The i2Coalition's main purpose in its comments is to add the perspectives and knowledge of its members to the record, not to scrutinize the legal foundations of the Proposed Rule. However, even a cursory scan reveals serious legal defects in both the procedural and substantive validity of the Proposed Rule.

    - *First*, as noted above, the lack of evidence on the effectiveness of the Proposed Rule and the failure to consider costs raise serious concerns about the validity of the Proposed Rule under the Administrative Procedure Act's ("APA") bedrock requirement that agency rules not be arbitrary and capricious.

    - *Second,* there is significant doubt as to the legal authority of the Department under the International Emergency Economic Powers Act to regulate transactions

[3] KYC in 2022, a Final Frontier for Digital Transformation in Financial Services, by Fenergo, *available at* https://resources.fenergo.com/reports/kyc-in-2022#main-content

entirely among U.S. persons or to regulate the transmission of information, both of which sit at the center of the Proposed Rule.

- *Third,* the NPRM's plan to issue "technical standards" that will determine the legal obligations of IaaS providers with respect to large artificial intelligence models through Federal Register publication, without notice-and-comment rulemaking, is inconsistent with the requirement that agency rules that have binding legal effect must go through the procedures set out in the APA.

These flaws are not only serious but are woven deep in the fabric of the Proposed Rule and EO 13984's entire notion that customer information collection helps solve the problem. The i2Coalition respectfully submits that the Department should withdraw the Proposed Rule and consider alternative strategies that are more likely to be effective. The i2Coalition recognizes the urgent need to address cybersecurity threats and how U.S. IaaS can be hardened against these threats. There have been and continue to be ongoing efforts in both government and industry to do so. Among these efforts has been the recent review and report of the President's NSTAC, which concluded unambiguously that:

> A requirement for IaaS providers to verify the identity of foreign customers (i.e., KYC) through collection and retention of national identification information and other information as proposed by EO 13984 would be unlikely to decrease [abuse of domestic infrastructure] by malicious foreign actors using domestic infrastructure. Further, such requirements may result in additional unintended consequences, including increasing friction with key U.S. allies, whose cooperation is critical in addressing global cyber threats.[4]

The Department should encourage the ongoing work to develop best practices that can be adopted widely across the Internet ecosystem.

---

[4] The President's National Security Telecommunications Advisory Committee, *Report to the President Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors*, at ES-4 (Sept. 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 ("NSTAC Report").

Active, technology-forward strategies that enable IaaS providers to prevent, detect, and deter malicious cyberactivity, and empower Internet users to protect themselves against attacks, hold the most promise. Purely passive, bureaucratic strategies that rely on casting wide dragnets for personal information are, at best, backwards looking and ineffective and, at worst, counterproductive and wasteful. Securing the domestic Internet infrastructure is important, but the Department should not and cannot require everyone in effect to get a license to use the Internet.

II. THE DEPARTMENT SHOULD FURTHER DEVELOP THE RECORD AND REFINE KEY CONCEPTS BEFORE ADOPTING ANY NEW REQUIREMENTS.

The Department should not promulgate the Proposed Rule because the scope and the substantive requirements are fatally underdeveloped and would prove impracticable both to comply with and enforce. As discussed in this Part, the Proposed Rule currently contains unworkably vague definitions and standards based on a paper-thin record that does not provide the Department or commenters enough information about the IaaS market, how different types of services fit into the broader Internet ecosystem, and how CIP requirements would be implemented. Instead of pushing out a rule that is enormously burdensome and ineffective, the Department should develop a much more robust record and seek industry input on practical, effective ways to achieve the Executive Orders' stated goals.

A. "Infrastructure as a Service Product," as Defined in the Proposed Rule, Lacks a Coherent and Rational Scope.

The ill-defined boundaries of what constitutes an "infrastructure as a service product" (or IaaS product) present a fatal deficiency in the Proposed Rule. The general vagueness of key terms in the definition is made worse by commentary in the NPRM that appears to directly contradict the definition in the proposed regulations. The regulatory impact analysis further shows that the proposed scope of an IaaS product is fundamentally mismatched with the reality

of who the providers are. Without a clear definition of the services being regulated, participants in the Internet ecosystem cannot know what their legal responsibilities are, much less ensure compliance with those responsibilities.

First, the text of the proposed regulation at 15 C.F.R. § 7.301 defines "Infrastructure as a Service product" as "a 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."[5] The Proposed Rule does not, however, set out what "software that is not predefined" means, but merely gives two non-exhaustive examples of overly broad categories of software in "operating systems and applications" while providing no definition for "predefined."

The term "software" is, on its face, extraordinarily broad. A National Institute of Standards and Technology definition provides that software is a "[c]omputer program[] and associated data that may be dynamically written or modified during execution."[6] The limiting criterion in the definition, that the software is "not predefined," is also subject to a wide range of reasonable interpretations, the broader ends of which would sweep in categories of products and services that bear no rational relationship to the stated purpose of the Proposed Rule to deter malicious cyber activities. For example, some commenters on the definition have argued that web hosting services and domain name registration services constitute IaaS products because

---

5 NPRM, 89 Fed. Reg. at 5726.

6 *Security and Privacy Controls for Information Systems and Organizations*, NIST Special Pub. 800-53 Rev. 5, at 419 (Sept. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

they meet the definition's requirements, including that the software is not "predefined."[7] Under this interpretation, every blog-hosting platform would be an IaaS product, and thus providers would have to require every person who wishes to create a blog to submit to the customer identification program. As computing power moves increasingly into the cloud, requiring a customer identification program for such a wide range of services will increasingly force providers to verify the identity of customers for everyday computing applications.

Second, commentary in the NPRM expands on the textual definition by identifying some specific services—but not others—that the Department deems to be IaaS products, including specifically "content delivery networks, proxy services, and domain name resolution services."[8] However, the NPRM does not provide any references or definitions for what these terms mean, which in common usage can apply to a wide variety of services that may or may not meet the definition of an IaaS product in the proposed regulation. For example, if the Department considers a virtual private network to be a "proxy service," that implies VPNs could be IaaS products, even though they do not provide users with any computing resources that give the ability to deploy software that is not predefined and thus fall outside of the definition in the proposed regulation. VPNs provide secure and private passage for data over the Internet that encrypts users' Internet traffic and protects it from third parties. They do not provide computing resources for deploying and running software that is not predefined, or give users control over operating systems, storage capacities, or deployed applications. Customer interactions with the provider's servers are highly limited to specific, predefined service configurations, such as server location.

---

[7] *See, e.g.*, Comments of Motion Picture Association, Inc., at 3, 5, Docket No. DOC-2021-0007 (filed Feb. 9, 2022) ("MPA Comments").

[8] NPRM, 89 Fed. Reg. at 5702.

Likewise, content delivery networks and domain resolution services do not provide the capability to deploy software that is not predefined, and the NPRM does not point to any evidence in the record showing otherwise. Content delivery networks cache content close to end users, reducing load times and Internet congestion for all users. Although customers can designate what content is cached, they cannot in any meaningful way "deploy" and "run software," such as executable applications or operating systems. To the extent customers of content delivery networks cache applications, the applications are for the use of the third-party customers, not of the entity purchasing services on the content delivery network. Moreover, if the mere capability to store and transmit *any* user-defined code constitutes an IaaS product, then every email service, messaging service, and cloud storage service would come within that definition, expanding its scope to cover dozens of services that nearly every American uses in everyday life.

Attempts in the NPRM to distinguish between related products further confuse the intended scope. The NPRM specifically concludes that, as applied to the domain name system ("DNS"), IaaS product does *not* include "domain name registration services for which a consumer registers a specific domain name with a third party, as that third party does not provide any processing, storage, network, or other fundamental computing resource to the consumer," but *does* include "domain name resolution services."[9] However, it provides no evidence or analysis distinguishing these two services, which are functionally connected and serve the same purpose of enabling Internet navigation.

Moreover, as discussed further below, the NPRM ignores how these and other Internet services are actually sold to their users. The Proposed Rule sweeps in all "resellers" of U.S. IaaS

[9] *Id.* at 5702.

products, which, in practice, would mean that the group provider the NPRM expressly carves out—domain registrars—would most likely be included as resellers of registry services. This confusion requires clarification that the performance of domain name resolution services as part of a domain name registration service does not make the latter an IaaS product.

Third, the NPRM's own regulatory impact analysis confirms that "infrastructure as a service product" has a confused and contradictory definition. That analysis sets a low estimate of 25 entities that would fall within the definition of a provider of IaaS products, but this is an implausibly small number given the expansive definition and commentary in the NPRM. Conversely, in the initial regulatory flexibility analysis, the NPRM uses the "roughly 1,800 enterprises categorized as 'Telecommunications Resellers' under NAISC Code 517911" as the starting point for determining how many small entities are likely to be impacted, while also acknowledging that the Department does not have data "on the number of these Telecommunications Resellers that offer IaaS products."[10] However, the definition of "IaaS product" much more closely matches the entities under the Computing Infrastructure Providers, Data Processing, Web Hosting, and Related Services category (NAICS Code 518210), which includes entities that are "primarily engaged in providing infrastructure for hosting or data processing services"[11] and has over 17,000 entities according to 2021 Census Bureau data.[12]

The fact that the number of entities potentially covered by the Proposed Rule could vary by three orders of magnitude underscores the underlying incoherence of the definition of IaaS product. Without a clear definition, a far larger number of providers that do not consider their

---

10 *Id.* at 5724.

11 *See NAISC Code Description 518210 - Data Processing, Hosting, and Related Services*, NAISC ASS'N, https://www.naics.com/naics-code-description/?code=518210&v=2017.

12 *See* U.S. CENSUS BUREAU, https://data.census.gov/table?q=518210.

own services to be IaaS products would be subject to the Proposed Rule. That also means that the resources needed by the Department to monitor compliance will vastly exceed the NPRM's estimate of two full-time employees, which would also undermine any potential effectiveness of the Proposed Rule. The Department should build a more robust record to develop and support a more targeted proposal that would help achieve the goals stated in the NPRM.

B. The Proposed Rule Provides Insufficient Standards on What a Compliant, "Risk-Based" Customer Identification Program Would Require.

The NPRM emphasizes that the Proposed Rule permits IaaS providers to adopt "risk-based" customer identification programs that do not create an undue burden. The i2Coalition agrees that regulatory obligations should take risk into account. Unfortunately, the Proposed Rule offers no workable standard by which providers can determine whether any CIP procedure, short of extensive, document-based verification of every single potential customer, would comply with its regulatory obligations. Faced with potential civil liability of up to $250,000 per violation,[13] providers will feel enormous pressure to err on the side of caution and adopt overly burdensome compliance programs.

The Proposed Rule defines "risk-based" as being "based on an appropriate assessment of the relevant risks, including those presented by the various types of service offerings maintained by the provider, the methods used to open an Account, the varying types of identifying information available to the provider, and the provider's customer base."[14] But this omits, crucially, any standard by which to weigh any particular risk profile for service, account type, and customer, against the series of steps that the provider must take to remain in compliance. For example, the Proposed Rule does not give any guidance on what information would be

[13] NPRM, 89 Fed. Reg. at 5735.

[14] *Id.* at 5727.

sufficient for a provider to definitively conclude that a potential individual customer is a U.S. person, even if the IaaS product at issue has minimal computing power and presents a vanishingly low risk of actual abuse. Likewise, there is no standard for when providers can determine the number of beneficial owners of a U.S. entity short of requiring non-public ownership information in each instance. In both examples, even assuming that the provider is able to require each potential customer to answer the question, the Proposed Rule does not give the provider any assurance that it can rely on the customer's answer without conducting further investigation to verify those answers.

Before promulgating a rule without a standard for measuring compliance, the Department should work with industry to develop a set of standards that will enable providers, including smaller businesses without large compliance teams and resources to engage outside professionals, to comply with the CIP requirements. These standards should, at a minimum, set out criteria for determining the risk level of a given service based on relevant factors, such as the level of computing power and the likelihood that it could be used for malicious ends.

C. The Proposed Rule's Definition of "United States Infrastructure as a Service Provider" Ignores Market Realities on Customer Information Access.

The Proposed Rule applies the CIP and reporting requirements to all U.S. IaaS providers, which are defined as U.S. persons that are "direct provider[s]" of IaaS products and "any of their U.S. resellers," as well as all foreign resellers of U.S. IaaS products.[15] Both the "direct providers," which presumably mean the entities that own and operate the facilities and equipment for "processing, storage, networks, or other fundamental computing resources,"[16] and the resellers are required to maintain CIPs that, at a minimum, "contain procedures for opening

[15] *Id.* at 5703.

[16] *Id.* at 5726.

an Account that specify the identifying information that will be obtained from each potential customer and beneficial owner(s) of an Account that will be used to determine whether they are U.S. persons."[17] However, resellers and "direct" sellers occupy very different positions in the value chain, such that it is unlikely that all entities in the chain have access to the same customer data required to comply with the Proposed Rule.

For example, all IaaS providers are required to collect contact and payment information from "any potential foreign customer or foreign beneficial owner prior to opening an Account," which is to say, *every* potential customer. However, depending on the particular distribution channel for a service, there may be no reason for the underlying infrastructure owner to possess, much less collect, payment and contact information from the customer in the first instance, as it may be the *reseller* who has the customer relationship and is responsible for collecting payment. Indeed, customer information is often a highly guarded, valuable asset of resellers, and requiring them to share that information with their underlying supplier in order for the supplier to be compliant with the Proposed Rule would cause significant commercial harm.

The Department should also clarify that a Reseller Account includes only those IaaS products that were purchased by the reseller for purposes of resale with the express authorization of the provider and contain only the capabilities of those IaaS products. This limitation means that entities that purchase IaaS products for use in creating their own services or products, which are not themselves IaaS products, are *not* within the definition of a reseller. For example, an entity that purchases server capacity for use in creating a cloud-based application for its customer to use and interact with, and which includes the capability for the end user to upload information,

[17] *Id.* at 5727–5728.

but with which they cannot deploy non-predefined software, would not be a reseller of IaaS products.

As the Department is developing a more targeted definition of IaaS product, it should also analyze and take into account the market structure and distribution models for those products to avoid or minimize imposing impracticable obligations. This will require more finely tuned divisions of responsibility between different parts of the value chain, rather than the attempted one-size-fits-all approach in the NPRM. Adopting premature rules would create confusion in the market that would make it difficult for customers to access the Internet services they need.

D. The Department Should Promote the Development of Industry-Vetted Abuse of IaaS Products Deterrence Programs Before Implementing the Proposed Rule.

The NPRM acknowledges that exemptions from the CIP requirements may be appropriate for specific types of "Accounts," customers, or specific IaaS providers if there are alternative means to deter abuse of U.S. IaaS products.[18] However, the Proposed Rule's procedures do not provide actionable guidance to potentially regulated entities on how to obtain such an exemption, and the proposed substantive requirements for an "Abuse of IaaS Products Deterrence Program" ("ADP") are both so extensive and vague that compliance with the ADP would likely be more burdensome than compliance with the CIP requirements themselves, and thus may disincentivize adoption of effective security measures. For example, the Proposed Rule requires ADPs to include "reasonable policies and procedures to . . . [i]dentify relevant Red Flags" indicating possible existence of "malicious cyber-enabled activities," but also states that such procedures will consider a list of enumerated "risk factors" that include, among other

[18] *See id.* at 5705.

things, the "[p]resentation of suspicious personally identifiable information or identity evidence."[19] The requirement to consider this "risk factor" appears to assume that providers will in the ordinary course collect "personally identifiable information or identity evidence" from their customers, which raises all the same issues of the CIPs and negates the benefit of the "exemption."

The Proposed Rule also does not provide any guidance on how providers can obtain an exemption, the timeframes for when such exemptions are to be evaluated, the potential bases for revocation, and gives the Department unfettered discretion to grant, deny, and revoke them. These uncertainties undercut any incentive on the part of providers to invest likely significant time and resources needed to develop and implement an ADP, as there is no reason for providers to think they can rely on the process or the outcome. The i2Coalition acknowledges that, given the nature of cybersecurity threats, effective ADPs need to be flexible and evolve with technology and behaviors. But that is all the more reason to avoid imposing prescriptive compliance requirements and instead encourage industry to continue to develop best practices and then use regulatory incentives to the extent still necessary for providers to adopt those practices.

IaaS providers already have extensive experience implementing fraud and abuse detection programs that attempt to account for the risks described in the NPRM. Working with industry, the Department should develop ways to evaluate the effectiveness of these existing efforts in curbing malicious activity and define additional best practices to help keep abuse of services at bay. The NSTAC Report expressly recommended that implementation of a CIP requirement be delayed and considered for "potential implementation" only after the

[19] *See id.* at 5730–5731.

development of "a framework that outlines best practices to mitigate" abuses of IaaS products.[20] Consistent with that recommendation, the i2Coalition urges the Department not to promulgate the Proposed Rule until it has identified a set of best practices that are more likely to be effective at deterring abuse of IaaS products.

E. The Proposed Rule Does Not Provide Any Workable Standard for the "Covered Transaction" Reporting Requirement.

Apart from the CIP requirements, the Proposed Rule also requires IaaS providers to report to the Department on all "covered transactions" of which they have "knowledge," where a covered transaction is defined to mean one between foreign persons and U.S. IaaS providers that involve or could involve "the training of a large AI model with potential capabilities that could be used in malicious cyber-enabled activity."[21] This requirement imposes an impracticable obligation on IaaS providers that is based on an unworkable standard in at least two critical ways.

First, there is no substantive definition for what constitutes a "covered transaction" such that IaaS providers can determine what needs to be reported because the Proposed Rule does not specify what it means to be "a large AI model with potential capabilities that could be used in malicious cyber-enabled activity." The NPRM notes that the Department will, at an unspecified later date, publish in the Federal Register "interpretive rules" containing the "technical conditions, based on technological advancements, as necessary and appropriate" to determine what constitutes such an AI model.[22] The Proposed Rule states only that the AI have "capabilities that could be used *to aid* or automate *aspects* of malicious cyber-enabled

---

[20] NSTAC Report at ES-6, 26.

[21] NPRM, 89 Fed. Reg. at 5729, 5733.

[22] *Id.* at 5706.

activit[ies]."[23] This definition does not give providers any way to distinguish between an AI model that is or is not covered by the rule, as *any* AI model in the hands of a bad actor could be capable of aiding aspects of malicious activities, which could be something as simple as generating phone numbers to dial or recombining text. To comply with this definition, IaaS providers would have to treat every transaction involving a foreign customer and any AI model as a "covered transaction."

Recognizing this untenable result, the NPRM states that the technical standard that would be used to determine whether any given AI model meets the definition, and thus triggering the legal obligations under the Proposed Rule, would be published separately in the Federal Register as an "interpretive rule." Presumably, by labeling these standards as interpretive rules, the Department does not intend to make them available for notice and comment. This approach would not only produce uninformed and unworkable standards but raises substantive and procedural concerns under the Administrative Procedure Act ("APA"), as discussed below. Instead, the Department should delay promulgating the Proposed Rule, with respect to AI models, until it has identified the applicable technical standards and made those available for notice and comment, consistent with the APA.

Second, the Proposed Rule's requirement that IaaS providers report covered transactions of which they have either actual or constructive knowledge assumes a degree of visibility into customers' usage of their resources that is not practicable.[24] IaaS providers do not have the means to monitor customer workloads hosted on their distributed network of servers, and thus

---

[23] *Id.* at 5727 (emphasis added).

[24] *See id.* at 5702 (defining "knowledge" as "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").

have no way of knowing when customers are using those resources to train any AI model, much less knowing whether such an AI model meets the as yet unknown technical specifications. Providers would thus have to rely on the customer to self-report whether their AI training run meets this technical standard, but the Proposed Rule makes no allowances for such reliance and presumes that providers can both actively monitor and interpret the software customers are running on their servers. Even if providers had the ability and resources to monitor the software being run, they, being IaaS providers and not artificial intelligence companies, likely do not have the personnel with the adequate knowledge and training to be able to determine whether any given piece of software meets the technical conditions to be published by the Department.

The i2Coalition appreciates the importance of having rules and incentives in place to guard against the misuse of powerful AI tools and encourages the Department to continue working with industry to identify and promote best practices actively preventing, detecting, and deterring such abuse while keeping pace with the speed at which this technology is developing. If at a future point there is evidence that regulation is necessary for specifically identified capabilities, then the Department should conduct a rulemaking proceeding consistent with the APA so that it can develop evidence-based, targeted rules that have a likelihood of success.

III. THE PROPOSED RULE IS ARBITRARILY OVERBROAD AND WOULD CREATE HARMFUL UNINTENDED CONSEQUENCES WITHOUT IMPROVING SECURITY.

As discussed in Part II above, major components of the Proposed Rule are so vague or indefinite that they do not provide any meaningful guidance to providers on how to comply. Adopting the Proposed Rule would impose significant compliance burdens on a very wide range of participants in the Internet ecosystem and harm not only industry participants but also expose ordinary, law-abiding users of the Internet to greater security risks. To do so on a record that

lacks any evidence that these requirements would promote the goals cited in the NPRM would be an arbitrary and capricious act.

A. The Scope of the Proposed Rule Is Effectively Unlimited for Internet Services and Imposes Significant Burdens on Providers that Bear No Rational Connection to the Stated Purposes of the Proposed Rule.

The scope of the Proposed Rule is wildly overbroad in at least three significant ways. First, it bears reemphasizing that the definition of "IaaS product" and the NPRM's interpretation thereof encompasses providers far beyond those that provide "infrastructure" capable of being used to commit malicious cyberactivity or train large AI models that threaten the national security of the United States. As discussed above, the Proposed Rule contains broad, undefined terms, including "software" and "predefined," in setting the boundaries of what constitutes an "IaaS product," which can be broadly construed to include virtually all products and services that enable users to upload content to the Internet. Indeed, one commenter writing in support of that expansive definition has applied it to all services that enable the implementation of "HTML, URL and HTTP(S)," reverse proxies, content delivery networks, all domain registration services, all domain name servers, online advertising services, and online payment processors.[25] Although the i2Coalition strongly disagrees with this expansive interpretation, the Proposed Rule's casual use of facially broad, undefined terms does not do enough to conclusively rule out such sweeping interpretations. The risk of civil or even criminal sanctions will pressure responsible providers to take a cautious approach and read the definition of "IaaS product" broadly.

Second, the "minimum" CIP as described in the Proposed Rule, far from actually accounting for risks related to malicious cyber activities, would require personal information collection from every person seeking to do something as simple as starting a blog or creating a

[25] *See* MPA Comments at 3-8.

cloud storage folder to share family photos, since these platforms are capable of being used to "store" or "process" non-predefined software. The Proposed Rule requires IaaS providers to obtain "at a minimum" information for "any *potential* foreign customer or foreign beneficial owner,"[26] such as their full legal name, residential address, payment information, telephone number, and IP addresses "used for access or administration and the date and time of each such access or administrative action, related to ongoing verification of such foreign person's ownership or control of such Account."[27] Because providers must "verif[y]" Accounts as belonging to U.S. persons with no foreign beneficial owners in order to avoid the CIP and records retention requirements,[28] providers necessarily must verify the *identity* of *every* potential customer and all of their beneficial owners in order to be certain that they are not in violation of the Proposed Rule.

Third, the Proposed Rule's vague and internally inconsistent treatment of resellers (or Resellers) of IaaS products will cause significant confusion for providers of all kinds of Internet-enabled services that may incorporate functionalities that fit into the broad definition of an "IaaS product." As discussed above, the Proposed Rule does not define who counts as a "reseller" of IaaS products but would impose the same CIP obligations on all such resellers. IaaS products, as they are broadly defined in the Proposed Rule, are inputs in a vast variety of services provided over the Internet. The Proposed Rule specifically defines "Reseller Accounts" and describes the

---

26 *See* NPRM, 89 Fed. Reg. at 5727 (emphasis added).

27 *See id.* at 5728.

28 *See id.* at 5728 ("If the IaaS provider verifies, through the procedures outlined in paragraphs (d)(2)(i) through (iii) of this section, that the customer and all beneficial owners are U.S. persons, the Account will not be subject to any other regulation in this subpart."); *see id* ("The CIP must contain procedures for verifying the identity of the potential foreign customer and beneficial owners of the Account, including by using information obtained in accordance with paragraph (d)(1) of this section, prior to opening the Account.").

resale of all or a portion of the purchased IaaS product and the selling of "those products" to a third party. But the Proposed Rule does not provide any guidance on when a combination of purchased IaaS capability with other functions or content ceases to be a resale of "that product" and becomes instead a different integrated service not subject to the Proposed Rule.

Moreover, the Proposed Rule uses the generic term "reseller" in the context of CIP obligations, so it is far from clear that the limitations contained in the definition of a Reseller Account even applies. Without a clear definition, "resellers" could include any provider of a web-based application or service that enables an end user to submit information, all of which is, by definition, encoded in "software," even if the service itself is being provided for other purposes. This could include websites that enable users to upload resumes or other documents to be processed, reviewed, or distributed; to upload images for publication or reverse searches; or even to comment in a free-form text box.

B. The Proposed Rule Hurts the Competitiveness of U.S. Companies and Undermines Internet Openness and Safety for Law-Abiding Users.

The sweeping scope of the Proposed Rule will greatly increase compliance costs for U.S. IaaS providers and drive away both U.S. and non-U.S. customers for their services. This will both hurt the competitiveness of U.S. companies and undermine Internet openness and safety by discouraging users from signing up for services that improve their own security on the Internet.

1. The NPRM Vastly Underestimates the Costs and Burdens of Compliance.

If the Proposed Rules were to be adopted, the cost of compliance for a large number of U.S. companies will likely be massive and far greater than the unrealistic estimates in the regulatory impact analysis accompanying the NPRM. First, as discussed above, the number of entities that will be covered by the Proposed Rule, whether intended targets or those who comply out of caution, will be far greater than the estimate in the NPRM.

Second, and relatedly, the NPRM vastly underestimates the number of new accounts each year that will be subject to verification by the service providers subject to the Proposed Rule. Without any support, the NPRM estimates that the Proposed Rule will impact anywhere between 100 and 1,000 new accounts for each entity subject to the Proposed Rule. To the extent the Proposed Rule applies to web hosting services and CDNs, it would be triggered every time a new website signs up for services with a U.S. provider. With nearly 200 million estimated websites that are live on the Internet at any given time,[29] the number of new accounts subject to the Proposed Rule's identity verification requirement would be many orders of magnitude greater than the Department estimates. And if the Proposed Rule were to apply to VPNs, as suggested in the NPRM's commentary, the number of new accounts subject to the requirements would be multiples larger, with billions of people using VPNs worldwide.[30]

Third, the NPRM does not consider all the costs that providers will have to incur to change their existing processes in order to comply with the Proposed Rule. Implementing CIP will require providers to set up entirely new compliance teams to develop, implement, and maintain identity verification processes. While the Department estimates a provider will spend 330 hours a year (less than 1 hour a day) implementing a CIP, in reality, the costs and resources will be significantly higher. Financial institutions have entire teams dedicated to KYC and expend considerable resources on their programs. In the 2022 survey of global banks, 97% of banks reported having teams ranging from 500 to 3,000 full-time employees managing their

---

[29] *See, e.g.*, Katherine Haan, *Top Website Statistics for 2024*, FORBES (Apr. 2, 2024), https://www.forbes.com/advisor/business/software/website-statistics/.

[30] *See, e.g.*, Chauncey Crail, *VPN Statistics and Trends in 2024*, FORBES (Feb. 29, 2024), https://www.forbes.com/advisor/business/vpn-statistics/#:~:text=1.6%20Billion%20People%20Use%20VPNs%20Throughout%20the%20World.

KYC programs, with the majority of banks conducting between 2,000 and 4,000 KYC events per month.[31]

The NPRM also completely ignores the difficulty of implementing identity verification processes, which will necessarily be required in order for the provider to be able to determine that any given individual customer is not a foreign person. Many companies do not collect the extensive list of personal information at sign up. At most, providers' current systems collect information from customers upon sign up to facilitate payments and invoicing. These systems were not engineered to collect or validate identity documents and live images for comparison. In order to verify documentary evidence, providers would have to contract with and onboard an identity verification vendor, and then work to integrate that verification process into the existing customer onboarding flow. Doing so requires extensive engineering of the entire sign-up flow, which is resource and time intensive, and will potentially interfere with existing business product launch roadmaps and other revenue generating activities. By one estimate conducted by an i2Coalition member, for smaller companies, standing up a CIP alone could take at least a year of dedicated engineering work and a cost upwards of $1 million. They will also need to set up additional secure systems to retain large amounts of highly sensitive personal and commercial information for years, even after a customer closes their account. None of these costs are accounted for or considered in the NPRM or regulatory impact analysis.

The compliance burden for sales to enterprise customers will be even greater because of the requirement not only to collect but also to verify and update information about all beneficial owners. Currently, service providers rarely, if ever, ask for information about beneficial owners,

---

[31] KYC in 2022, a Final Frontier for Digital Transformation in Financial Services, *available at* https://resources.fenergo.com/reports/kyc-in-2022#main-content

especially non-controlling minority investors that hold as little as 25% of the interest in the customer. Ownership information for entities is not publicly available and, in many cases, is highly commercially sensitive and valuable. Even for publicly traded companies, the only information publicly available relates to direct shareholders, and the Proposed Rule would require identity verification for persons who "own[] or control[] at least 25 percent of the ownership interests of a customer,"[32] which, on its face, would include at least one indirect ownership tier (i.e., persons who "control" the entity that owns a 25% stake). Given the sensitivity of this information, it will be exceedingly difficult for service providers to be able to obtain such information from their customers, which they then would have to verify.

Moreover, providers must also have "procedures" to "require a customer to notify the IaaS provider of any changes in the customer's ownership—such as adding or removing beneficial owners—and the IaaS provider's process for ongoing verification of the accuracy of the information provided by a customer."[33] Included among the beneficial ownership information subject to ongoing updating and verification is all of the information required to be collected at account creation, including physical addresses and IP addresses "related to ongoing verification of such foreign person's ownership."[34] Full compliance with these requirements will, in all likelihood, be practically impossible. Yet the Proposed Rule does not contain any intelligible standard or safe harbors for risk assessment that providers can rely on to know the circumstances in which they would *not* need to obtain all of the information necessary for identity verification.

---

[32] NPRM, 89 Fed. Reg. at 5726.

[33] *Id.* at 5729.

[34] *Id.* at 5728.

The reseller requirements could also force many IaaS providers to change their distributor and reseller relationships so that the parties will all have the information needed to comply with the Proposed Rule, even if this creates commercial inefficiencies or outright conflicts-of-interest between infrastructure owners and their distributors and resellers. For example, as noted above, customer account and contact information are highly commercially-valuable data for resellers, who would risk undercutting their own business by providing these to the infrastructure owners.

Large and resourceful entities may, over time, figure out ways to comply with these requirements, but only at an enormous expense and disruption to their businesses. Yet even these companies do not have infinite resources, and all of the time and money spent on creating the vast personal information collection machinery needed to comply with the Proposed Rule will not be available for activities that actually prevent, detect, and deter malicious cyber activity. The record shows that IaaS providers use a variety of strategies, including "automated processes to analyze metadata and compare account usage to historical behavior" and other tools based on real-world experience with malicious actors.[35] Many of these activities are resource-intensive and require constant updates and changes to match the evolving threat. As the Information Technology Industry Council explained, providers "employ dedicated teams of experts, as well as technical and analytics mechanisms that complement their efforts to look for indications of malicious use."[36] Diverting resources to focus on the CIP requirements will thus also increase risks and costs for providers by potentially reducing the effectiveness of their active prevention systems.

---

[35] *See* Comments of the Information Technology Industry Council at 5-6, Docket No. 210913-0183, DOC-2021-0007 (filed Oct. 25, 2021) ("ITIC Comments"); *see also* Comments of Microsoft Corp. at 3–4, Docket No. 210913-0183, DOC-2021-0007 (filed Oct. 25, 2021) (describing proactive strategies to prevent abuse of U.S. IaaS).

[36] ITIC Comments at 5.

Smaller providers without the legal, compliance, finance, engineering, and IT heft of their larger counterparts will face a much more difficult challenge and expose themselves to far greater legal risk. Creating different CIPs for every single provider creates a large amount of inefficiency and waste, but providers have no alternative because the Proposed Rule does not provide any reliable guidance on what kinds of "risk-based" CIPs will be acceptable. Thus, responsible IaaS providers and other companies potentially within the scope of the Proposed Rule will err on the side of caution and implement extensive CIPs that will require all potential customers to turn over highly sensitive information in order to purchase or even just to try their products.

2. The Proposed Rule Will Require or Incentivize Behavior that Harms U.S. Companies' Competitiveness and Undermines Internet Openness and Security.

Internet users value their privacy. This observation is a truism and not just for those that wish to use the Internet to do harm. Ordinary, law-abiding people have perfectly legitimate reasons not to casually surrender their names, phone numbers, physical addresses, email addresses, and IP numbers. They may want to avoid receiving unsolicited communications, reduce the risk of getting their information stolen, or they may simply not like being watched.

Whatever the reason, imposing invasive CIP requirements across a wide range of Internet services will discourage people from using those services, will encourage them to provide false information, or will drive them to non-U.S. providers. This chilling effect will have a particularly harsh impact on Internet users who live under repressive regimes and rely on the privacy enabled by services, like VPNs and other proxies, and on forums, file storage, and transfer services. As most of these individuals will not be U.S. persons under the Proposed Rule, the intrusive identity verification requirements indisputably will apply to them, and if providers

are not able to verify identities, they may be required by the Proposed Rule to deny access to these individuals.

The behaviors that the Proposed Rule either mandates or strongly incentivizes will harm the Internet ecosystem. U.S. providers of IaaS products will immediately become less competitive compared to their non-U.S. competitors who do not have to reengineer their interfaces, systems, sales processes, and other commercial and technical aspects of their business simply to remain compliant with the law. This will make the competitors more attractive to customers both because they do not require the intrusive CIP processes and because their lower costs could translate into lower prices. The competitive impact is likely to be felt especially among those serving enterprise customers, who will have to provide and keep updated extensive and highly commercially sensitive ownership information, and will thus have a strong incentive to use non-U.S. providers. This distortion to competition will not only harm U.S. companies financially but will also undermine the very goals proffered by the NPRM as users shift to companies that may be either more vulnerable to cyberattacks or more susceptible to foreign government influence, or both.

Internet users will also be discouraged entirely from using services that currently improve their Internet security. This makes those end users' Internet usage more susceptible to unwanted private information collection, which in turn could increase the risk that their sensitive information is stolen or that their accounts get hijacked. As the NSTAC Report noted, CIP requirements can do "more harm than good" because "the identity-fraud market would expand to meet attackers' demand for seemingly legitimate user credentials and accounts."[37] If legitimate

[37] NSTAC Report at 23.

user accounts are easier to compromise, then CIP processes that apply at the point of account creation will become even less effective.

C. The Record Lacks Evidence that CIPs Advance Any of the Stated Purposes of the Proposed Rule.

There are no rational grounds based on the existing record for concluding that the high price paid by providers and users to comply with the Proposed Rule will result in any improvement to security. The record lacks any evidence that CIPs will have any effect on reducing the likelihood of abuse of U.S. IaaS products for malicious cyber activity or on improving national security. At a minimum, the Department must establish in the record evidence that shows both that the wide range of IaaS products as defined actually contributes to the harms the Proposed Rule seeks to reduce and that the methods in the Proposed Rule will mitigate those harms. The record shows neither.

First, there is no evidence of the rates at which the types of services and products that potentially fit into the broad definition of IaaS product have been abused to commit malicious cyber activity, or the degree to which their use by persons outside of the United States increases the risk of abuse. The NSTAC Report highlights the general lack of reliable evidence in this area, concluding that "the committee was not briefed on any rigorous studies analyzing the tradeoffs of potential policy and technical approach that attempt to distinguish between domestic and foreign abusers."[38] Given the lack of reliable data, the NSTAC Report concludes that CIP requirements "would be unlikely to decrease" abuses of IaaS "by malicious foreign actors."[39]

Indeed, the NPRM lacks not just evidence of harm but even a hypothesis for how IaaS products broadly defined enable malicious cyber activity. The NPRM states that IaaS products

[38] NSTAC Report at ES-4.

[39] *Id.*

enable customers to "run software and store data" and "commit intellectual property and sensitive data theft," that these perpetrators can "quickly move to replacement" services, and the "temporary registration and ease of replacement for such services makes it more difficult for the government to track malicious actors."[40] These observations are, of course, also true for any number of services and devices that enable access to the Internet, including personal computers and cellphones.

A malicious and capable person seeking to commit cybercrimes can buy an inexpensive used computer or cellphone and connect to any open WiFi access point to accomplish the tasks, and then easily swap out devices on the secondary market. If anything, IaaS products by their nature present a lower risk than a computer in the hands of such an individual precisely because the IaaS provider has control over the resources that would be used to commit the actions and can therefore implement systems to detect and prevent abuse. The NPRM provides no evidence or analysis on why IaaS products present either a unique or disproportionate risk.

Second, there is no evidence in the record that the CIP and related requirements in the Proposed Rule would do anything to reduce the risk of abuse of IaaS products to any appreciable degree beyond what companies are already doing. Determined malicious actors could simply use stolen credentials or identities to create an IaaS product account or utilize prevalent IP obfuscation services to mask their location. As the NSTAC Report noted, "most malicious actors route their cyber activities through at least one intermediary" and "those using virtual resources for legitimate purposes may become victims themselves, finding their infrastructure compromised for use in malicious activities."[41] Malicious actors could also "move their

---

[40] *See* NPRM, 89 Fed. Reg. at 5698.

[41] NSTAC Report at 1.

operations to non-cooperative virtual infrastructure providers located outside the U.S.,"[42] which would frustrate the considerable efforts that U.S. IaaS providers have already implemented. In the three years since this docket has been open, neither the Department nor the NSTAC has identified evidence that CIP rules and similar "such requirements . . . would be useful," or even that know-your-customer rules from the financial services industry, from which the CIP requirement borrows, provide a useful comparison.[43]

Given the absence of evidence justifying either the focus on U.S. IaaS products or the efficacy of CIP requirements, the Department should defer implementing the Proposed Rule and instead continue encouraging ongoing discussions between government agencies and industry participants to improve ways to prevent, detect, and deter abuse of IaaS products.

IV. THE PROPOSED RULE IS SUBSTANTIVELY AND PROCEDURALLY DEFECTIVE UNDER THE APA.

The Proposed Rule raises serious substantive and procedural concerns under the APA, and the Department should not promulgate a rule that is likely to be vacated on review.[44] First, Section 553 of the APA requires all agency rules to be subject to public notice and comment procedures except "interpretative rules and statements of policy."[45] Courts have consistently held that an "interpretive" rule does not have the force of law on its own but instead "derive[s] a proposition from an existing document whose meaning compels or logically justifies the

---

42 *Id.*

43 *Id.* at 23.

44 *See Holy Land Found. for Relief & Dev. v. Ashcroft*, 333 F.3d 156, 162 (D.C. Cir. 2003) (noting that agency implementation of International Emergency Economic Powers Act is subject to APA review).

45 5 U.S.C. § 553(d).

proposition."[46] In contrast to interpretive rules, "legislative" rules do carry the force of law and thus must follow the APA's notice-and-comment procedure.[47] Following this principle, any rule that "modifies or adds to a legal norm based on the agency's own authority" is a legislative rule.[48]

Under this well-established test, the to-be-published technical conditions for determining what will be a "large AI model with potential capabilities that could be used in malicious cyber-enabled activity" is clearly a legislative rule because it "modifies or adds" to the legal obligation of IaaS providers at the discretion of the Department.[49] Despite the characterization in the NPRM, these "technical conditions" also cannot be merely an interpretation of the Proposed Rule because the vague standard described above does not "compel[] or logically justif[y] the proposition" stated in the technical standards.[50] Courts have made clear that agencies cannot purport to interpret "vague or vacuous terms" as a way to avoid the requirements of the APA.[51] The APA's notice and comment process is especially important for this particular rule because it "is the procedure by which the persons affected by legislative rules are enabled to communicate

---

46 *Cath. Health Initiatives v. Sebelius*, 617 F.3d 490, 494 (D.C. Cir. 2010) (internal quotation marks omitted).

47 *See, e.g.*, *Ass'n of Flight Attendants-CWA, AFL-CIO v. Huerta*, 785 F.3d 710, 717 (D.C. Cir. 2015) ("The most important factor in differentiating between binding and nonbinding actions is the actual legal effect (or lack thereof) of the agency action in question." (internal quotation marks omitted)).

48 *Id.* at 716.

49 *See id.*

50 *See Cath. Health Initiatives*, 617 F.3d at 494 (internal quotation marks omitted).

51 *See id.* at 495; *see also United States v. Picciotto*, 875 F.2d 345, 348 (D.C. Cir. 1989) ("A reviewing court need not classify a rule as interpretive just because the agency says that it is.").

their concerns in a comprehensive and systematic fashion to the legislating agency."[52] Until the Department provides these "technical conditions," there is no way for potentially affected entities to provide their concerns in any manner.

Second, the Proposed Rule is inconsistent with Section 706 of the APA because it is arbitrary and capricious in its definition of what an IaaS product is and its expansive requirements on what IaaS providers must do to comply with the CIP requirements. For the reasons discussed above in Parts II and III, the NPRM "fails to provide comprehensible guidance"[53] on what constitutes an IaaS product because it does not define what constitutes "software that is not predefined." Without clear guidance to potentially affected entities or an intelligible limiting principle, the scope of the Proposed Rule is so broad and unmoored as to be arbitrary and capricious. The Proposed Rule's CIP requirement is also arbitrary and capricious for the reasons discussed in Parts II and III above because the Department has neither considered the full scale of the burden on regulated entities and the harm on Internet users, nor justified its Proposed Rule with substantial evidence that it will meaningfully reduce malicious cyberactivity. Because the Department "failed to consider an important aspect of the problem, [and] offered an explanation for its decision that runs counter to the evidence before the agency, or is so implausible that it could not be ascribed to a difference in view or the product of agency expertise," a reviewing court "should cast the action aside as arbitrary and capricious."[54]

---

[52] *Hoctor v. Dep't of Agric.*, 82 F.3d 165, 171 (7th Cir. 1996).

[53] *Hikvision USA, Inc. v. FCC*, 97 F.4th 938, 950 (D.C. Cir. 2024).

[54] *TikTok Inc. v. Trump*, 507 F. Supp. 3d 92, 111 (D.D.C. 2020) (quoting *Motor Vehicle Mfrs. Ass'n of U.S. Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983) (internal quotation marks omitted)).

Third, the Proposed Rule also raises Section 706 concerns because its purported regulation of purely domestic transactions and transmission of information is "in excess of statutory jurisdiction, authority, or limitation."[55] The IEEPA's grant of authority is expressly limited to "transactions involving[] any property in which any foreign country or a national thereof has any interest by any person, or with respect to any property, subject to the jurisdiction of the United States."[56] Importantly, this authority does not extend to transactions that "are not in themselves transactions involving [foreign] property or efforts to exercise rights with respect to such property."[57] The CIP requirements necessarily apply to entirely domestic transactions between U.S. person customers and IaaS provides. For the reasons discussed above, in Part III.A, IaaS providers must collect and retain information about all potential customers, including U.S. customers, in order to meet the Proposed Rule's requirement that they verify the identity of *potential* foreign customers. The Proposed Rule's regulation of transactions with no foreign nexus exceeds the authority conferred by Congress, and thus is inconsistent with the APA.

Fourth, the Proposed Rule also exceeds the authority granted by the IEEPA because that statute expressly excludes from regulation, either "directly or indirectly," the cross-border transmission of "information or informational materials."[58] The definition of IaaS product in the Proposed Rule, as discussed in Part II.A above, is so nebulous and broad that it includes the ability to transmit information, such as in services like proxy services and domain resolution services. The Proposed Rule is an indirect regulation of the cross-border transmission of

---

55 5 U.S.C. § 706(2)(C).

56 50 U.S.C. § 1702(a)(1)(B); *see also id*. § 1702(a)(1)(A)(ii) (delegation of the power to the President to regulate transfers of credit and payments "to the extent that such transfers or payments involve any interest of any foreign country or a national thereof.").

57 *Dames & Moore v. Regan*, 453 U.S. 654, 675 (1981).

58 50 U.S.C. § 1702(b)(3).

information because it significantly increases IaaS providers' costs of providing services to non-U.S. persons by, among other things, requiring identity verification for foreign nationals living abroad. Therefore, the Proposed Rule raises serious APA concerns by imposing regulations for which the Department lacks statutory authority.

V. AT A MINIMUM, THE DEPARTMENT SHOULD NARROW THE SCOPE OF THE RULE AND PROVIDE CLEAR SAFE HARBORS.

If the Department does decide to promulgate the Proposed Rule, despite the lack of evidentiary basis, it should at least take the following minimum steps to reduce unnecessary burdens imposed on the Internet ecosystem. These include narrowing the scope of what an "IaaS product" is, setting out clear safe harbors that are applicable to providers in implementing CIPs, and extending the implementation window to enable a smooth transition without harming Internet innovation and openness and disrupting the operations of scores of businesses and competition.

A. The Department Should Adopt More Precise Definitions for "Software" and "Predefined."

As discussed above, the current definition of an "IaaS product" is unclear and subject to expansive interpretation that exceeds any rational connection to the Executive Orders or the stated purpose of the Proposed Rule.[59] To address this issue, the Department should defer on promulgating any rule until it can develop an informed, coherent, limited, and useful definition of an "IaaS product." If, however, the Department does decide to promulgate the Proposed Rule, it should, at a minimum, define what constitutes "software that is not predefined" with greater precision based on an appropriate scope.

---

[59] *See supra* Part III.A.

In doing so, the Department should apply two limiting principles that are both based on the stated purposes of the Proposed Rule to aid law enforcement, prevent foreign persons from using U.S. IaaS products to conduct malicious cyber-enabled activities, and to safeguard the national security of the United States.[60] First, the Department should define "software" for purposes of this rule and limit it to software *applications* that can execute code capable of causing harm to other systems and networks. This would remove some ambiguity from the rule and narrow its scope without sacrificing any of the stated security benefits. Second, the Department should make clear that software that is not "predefined" means that the customer purchasing the service has complete control over the contents and capabilities of the software, and that the ability of the customer to select from a menu of pre-coded templates, scripts, modules, or application program interfaces does not constitute the ability to deploy software that is not predefined. This change would make clear, for example, that a blog-hosting platform that provides a suite of preset scripts, APIs, and other features does not constitute an IaaS product. Likewise, proxy and reverse proxy services would also not be included within the definition of an IaaS product because customers do not have the ability to deploy software that is not predefined.

B. The Department Should Set Out Clear Safe Harbors for Providers that Implement Risk-Based CIPs.

The NPRM emphasizes that IaaS providers should be able to develop and implement CIPs that are risk-based, but it does not provide any guidance on how to weigh those risks and, more importantly, does not provide companies with any assurance that their risk-based decisions will be deemed acceptable by the Department until it is too late to change them. This

[60] *See* NPRM, 89 Fed. Reg. at 5725.

combination of vague standards and lack of assurance of compliance will create confusion for providers.

To mitigate this issue and improve compliance, if the Department were to promulgate CIP requirements, it should also set out clear safe harbors for companies based on objective standards for risk. In other contexts in which a regulated entity must rely on information provided by another person to meet its own obligation, applicable regulations permit the entity to rely on customer statements.[61] IaaS providers likewise should be able to rely on the safe harbors for specific risk-based CIPs that are deemed to be compliant. The Department should seek further comment on what types of safe harbors are appropriate for risk-based CIPs. Each safe harbor provision should include a description of the requirements for the CIP based on specified risk factors.

i2Coalition urges the Department to at least adopt the following safe harbors for IaaS providers that have a policy and/or provisions in their customer agreements allowing the provider to suspend service if it has reason to believe that the customer is using the service for illegal activities or otherwise against the provider's acceptable use policies.

- For all IaaS products to the extent offered on a mass-market, retail basis, the CIP requirements do not apply. A mass-market retail IaaS product is one that is designed for, marketed primarily to, and set at price points targeted to individuals and small and medium size businesses rather than enterprise customers.
- For IaaS products that are not mass-market, retail offerings: (a) the providers' CIPs may deem that a potential customer is a U.S. person if: (i) the IP address used for signup is associated with a U.S. location, (ii) the billing address is a U.S. address, or (iii) the customer certifies that it is a U.S. person as defined in the Proposed Rule; and (b) the provider is not required to gather beneficial ownership information for any customer that

[61] *See, e.g.*, 47 C.F.R. 79.1(g)(7) ("Video programming distributors may rely on certifications from video programmers made in accordance with paragraph (m) of this section to demonstrate compliance . . . . Video programming distributors shall not be held responsible for situations where a video programmer falsely certifies . . . unless the video programming distributor knows or should have known that the certification is false.").

is a U.S. person. For example, a provider that treats a signup from any U.S. IP address as a U.S. person would meet the CIP requirement.

- For IaaS products that are not mass-market, retail offerings for which the potential customer is *not* a U.S. person and is an individual (or for beneficial owners who are individuals), the IaaS provider can rely on the individual's statement as to their identity without further verification *unless* the IaaS provider has specific reasons to believe that the individual's statement is false. For example, a provider that relies on a foreign person's certification as to their own identity, in the absence of affirmative evidence that the certification is untrue, would meet the CIP requirement.

- For IaaS products that are not mass-market, retail offerings for which the potential customer is *not* a U.S. person and is *not* an individual, the IaaS provider will be deemed to have satisfied the requirement to obtain beneficial ownership information so long as it has made at least two good-faith attempts to request such information from the customer (including by email) during and after initial sign-up, and on an annual basis thereafter.

C. The Department Should Provide Clear Guidance on the Process and Requirements for the Abuse of IaaS Products Deterrence Program Exemption

The NPRM proposes to adopt a process for exempting providers that comply with "security best practices to deter abuse of IaaS products" and have "established an Abuse of IaaS Products Deterrence Program (ADP)" from CIP requirements.[62] The i2Coalition appreciates this proposal and agrees that IaaS providers should be exempted from the CIP requirements if they are already mitigating risk appropriately. However, the Proposed Rule is unclear as to how providers can apply for and obtain the exemption, and what substantive standards they need to meet to qualify as having established an ADP. The i2Coalition respectfully requests that the Department clarify the specifics of the ADP exemptions in the following ways.

First, there should be a clear process and timeframe for the Department's review and decision making on an application. Currently, the Proposed Rule states that, after a provider submits an application, "the Secretary will review the submission and may request additional information from the submitter," and that "[p]rior to making a finding, the Secretary will consult

[62] NPRM, 89 Fed. Reg. at 5730.

with" certain other Executive Branch agencies before making a decision.[63] Providers will be in a much better position to plan business decisions—including the significant engineering work required to comply with the CIP requirements described in Part III.B above—if there were clearer guidance on the timelines for obtaining a determination on the ADP exemption. This, in turn, will increase incentives for providers to implement ADPs.

Second, the Department should set more detailed standards for how it will evaluate ADPs so that providers can design their programs accordingly. For example, the NPRM states that the Secretary will consider "[w]hether the ADP is an appropriate size and complexity commensurate with the nature and scope of product offerings."[64] Providers would be able to design their ADPs with more certainty if there were guidance on what risks or capabilities of specific IaaS products warrant more or less complex ADPs. Likewise, the Department should provide examples of specific "Red Flags" that should be accounted for by the ADP, of "reseller arrangements" that would be deemed to be effective, and specific "public-private collaborative efforts" in which providers should participate in order to qualify for the exemption.

Third, the Department should clarify the scope of the ADP exemption, specifically that: (1) a provider's ADP need apply only to that provider's IaaS products instead of more broadly to all of that provider's services; and (2) that an IaaS provider's exemption from the CIP requirements extend to all resellers of that provider's IaaS products. The first clarification is necessary for providers to be able to appropriately design their ADPs to suit the specific risks presented by IaaS products. The second clarification provides greater certainty for providers whose business models rely on multiple distribution channels in addition to direct sales.

---

63 *Id.* at 5732.

64 *Id.*

Fourth, the ADP exemption should contain clear guidelines for the standards and procedures for any proposed revocation of a granted exemption, including a process for appeal and review. The NPRM states that providers who have been granted ADP exemptions must notify the Department on "any significant deviations or changes to their ADP" and update their ADPs in response to "the changing threat landscape."[65] It further provides that the exemption "may be revoked at any time" by the Department.[66] However, the Proposed Rule contains no guidance or standards on the conditions that have to be met for the Department to revoke a granted exemption, the processes that the Department must follow in a revocation proceeding, or what protections and rights providers have to contest such proposed revocations. Without these essential details, the benefits of the ADP exemption seem more illusory than real.

D. IaaS Providers Should Be Able to Rely on Customer Certifications As to AI Models to Satisfy the Obligation to Report "Covered Transactions."

As discussed in Part II.E, the Proposed Rule's requirement that IaaS providers report all "covered transactions" of which they have actual or constructive knowledge fails to recognize the strict practical limits on providers' ability to monitor and interpret the software that customers run on their servers at a level of granularity required to determine whether the usage consists of training large AI models. The Department should make clear that providers can rely on their customers' self-certification as to whether their use of the server resources meets the definition of a "large AI model with potential capabilities that could be used in malicious cyber-enabled activity." IaaS providers do not otherwise have the resources or technical expertise needed to determine whether any customer transaction is a "covered transaction." To avoid effectively requiring reporting every transaction with a foreign customer as a "covered

---

65 *Id.*

66 *See id.*

transaction," the Department should adopt a safe harbor that allows providers to rely on the certifications of their customers with respect to whether their AI model meets the technical conditions specified by the Department.

VI. CONCLUSION

For the reasons set forth above, the Department should not rush out rules that would be ineffective at accomplishing the goals described in the NPRM, create significant disruption and harm to large parts of the Internet ecosystem, undermine the posture of U.S. companies in a highly competitive and rapidly evolving industry, deprive Internet users around the world of important security tools including those that enable them to resist oppressive regimes, and contain grave procedural and substantive defects under the APA.

Respectfully submitted,

Henry Shi

Henry Shi
HWG LLP
1919 M Street, NW, Suite 800
Washington, DC 20036
(202) 730-1348
hshi@hwglaw.com

Counsel for Internet Infrastructure Coalition

Christian Dawson
Ann Morton
Internet Infrastructure Coalition
2920 W Broad St. Suite 80
Richmond, VA 23230
dawson@i2coalition.com
ann@i2coalition.com

April 29, 2024