Before the
U.S. Department of Commerce
Bureau of Industry and Security
Washington, D.C.

In re Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities	Docket No. 240119–0020

COMMENTS OF
THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION (CCIA)

The Computer & Communications Industry Association ("CCIA")[1] submits the following comments in response to the Department of Commerce Notice of Proposed Rulemaking published in the Federal Register at 89 Fed. Reg. 5698 (January 29, 2024).[2]

CCIA is an international, not-for-profit trade association representing a broad array of communications and technology companies. For more than fifty years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy.

CCIA members are at the forefront of research and development in the technological fields of artificial intelligence and cybersecurity. CCIA members have also been recognized as security leaders of cloud infrastructure-as-a-service platform providers and have learned countless lessons regarding the benefits and challenges of this industry.[3] CCIA appreciates the opportunity to provide comments and consideration on how those lessons may be applied to address malicious cyber-enabled activities.

[1] A complete list of CCIA members is available at http://www.ccianet.org/members.
[2] 89 Fed. Reg. 5698 (January 29, 2024) (hereinafter "NPRM").
[3] Google Cloud, *Google named a Leader in Forrester Wave™ IaaS Platform Native Security*, Blog (April 26, 2023) https://cloud.google.com/blog/products/identity-security/google-named-leader-in-forrester-wave-iaas-platform-native-security.

I. Summary

CCIA and its members support the United States government's commitment to combating malicious cyber-enabled activity, including the security threats and potential risks associated with the abuse of domestic infrastructure by foreign malicious cyber actors. Improving the nation's cyber defense is a shared goal and our members, which include major U.S. infrastructure-as-a-service (IaaS) providers, continue to substantially invest in and improve their abuse detection and mitigation measures.

The 2023 National Cybersecurity Strategy reiterated the importance of building upon these mutually shared goals through the development of strong public-private partnerships. The Administration's sustained efforts to foster a collaborative approach have been essential to the success of these past initiatives but the NPRM greatly diverts from this approach and risks disrupting these successful partnerships. Furthermore, the Department's proposed regulations risk exceeding the rulemaking authority granted by Congress.

CCIA has serious concerns about the effectiveness of the proposed Customer Identification Program (CIP) in meeting the objectives listed in Executive Orders 13984 and 14028,[4] especially considering the implications to the privacy, security, and global competitiveness of U.S. IaaS providers. The proposed exemption process contains serious defects that threaten businesses' ability to obtain an exemption. These concerns also extend to the prescriptive AI model reporting requirements that will compromise the public's trust in U.S. IaaS providers. Taken together, the NPRM imposes costly requirements that will impede upon, if not restrict, the private sector's ability to prevent and deter the abuse of their services.

CCIA strongly urges the Department to reassess its proposed approach and shift its focus toward the adoption of the Abuse of IaaS Products Deterrence Program (ADP) as the primary method to address these concerns. This would align with the conclusions and recommendations described in the National Security Telecommunications Advisory Committee's (NSTAC) report on addressing the abuse of domestic infrastructure.[5] CCIA offers the following comments to

---

[4] EO 14028 largely focuses on improving the security posture of the U.S. government including strengthening the existing efforts addressing the concerns highlighted in EO 13984 but it also emphasized the importance of collaborating with the private sector to achieve these aims.

[5] National Security Telecommunications Advisory Committee, *NSTAC Report to the President: Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors*, (Sept. 26, 2023) (hereinafter "NSTAC Report") 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

ensure that any final Rule accounts for the impact on U.S. businesses, advances the government's goals, and effectively addresses the issues identified in the executive orders.

II. Rulemaking Authority

"Administrative agencies are creatures of statute. They accordingly possess only the authority that Congress has provided."[6] While we appreciate the intended aims of the NPRM to prevent malicious cyber-enabled activities, the Department's proposed regulations would exceed its rulemaking authority.

First, the Department would exceed its rulemaking authority by requiring U.S. IaaS providers and their foreign resellers to collect and retain the information associated with transactions involving only U.S. persons. To comply with CIP requirements, businesses would need to collect, verify, and maintain personal identifying information about any potential foreign customer. However, the overbreadth of the proposed rule would force providers and resellers to verify the information of *every actual or potential customer* as this would be the only way to determine whether a customer is a U.S. person or a foreign person.

Congress in passing the International Emergency Economic Powers Act (IEEPA) delegated broad authority to the President to regulate economic transactions following a declaration of national emergency.[7] IEEPA has placed several limits on this authority including excluding the regulation of transactions that "are not in themselves involving [foreign] property or efforts to exercise rights with respect to such property."[8] As a result, efforts to regulate transactions with no foreign nexus would exceed the authority delegated by Congress under IEEPA. The Department's proposed regulations would violate this limit on rulemaking authority as to avoid liability, companies would have to comply with all the requirements for any potential transactions even if it only involves U.S. persons. Further, businesses would need to retain this information in the event of a compliance review or audit.

Second, the Department violates an express limitation in IEEPA by regulating the transmission of information and informational materials. Congress amended IEEPA to expressly

---

[6] *Nat'l Fed'n of Indep. Bus. v. Dep't of Lab., Occupational Safety & Health Admin.*, 142 S. Ct. 661, 664 (2022); *see also Louisiana Pub. Serv. Comm'n v. FCC,* 476 U.S. 355, 374 (1986) ("an agency literally has no power to act … unless and until Congress confers power upon it").
[7] 50 U.S.C. § 1702(a)(1).
[8] *Dames & Moore v. Regan*, 453 U.S. 654, 675 (1981).

limit the President's authority to regulate information materials which broadly applies to all information "regardless of format or medium of transmission."[9] The 1994 House Conference report made clear that Congress intended both amendments "to facilitate transactions and activities incident to the flow of information and informational materials without regard to the type of information, its format, or means of transmission…"[10]

Here, the NPRM broadly defines covered IaaS products to include services that involve the transmission of content. The Department explains that the definition would broadly encompass "services such as content delivery networks, proxy services, and domain name resolution services."[11] By expanding the scope of the proposed rule, the Department would indirectly regulate the transmission of information across borders—in direct violation of the informational materials exception. The broad sweeping know-your-customer regulations proposed in the NPRM are likely to face significant legal challenges, which will undermine public and private efforts to implement the goals outlined in the executive orders. CCIA strongly urges the Department to reconsider the approach taken in the NPRM to ensure it adheres to the statutory limits established by Congress and actually advances its long-term objectives.

III. CIP Regulations and Relevant Exemptions

A. Privacy Considerations and Implications

One of the proposed CIP requirements is that it must contain procedures enabling a U.S. IaaS provider or their foreign reseller "to determine whether a potential customer and all beneficial owners are U.S. persons."[12] It is unclear how a provider is to comply with these requirements other than by collecting and retaining the personal information of all actual and potential customers and beneficial owners. These rigid requirements also impede businesses' efforts to implement more privacy-protective approaches for handling customer information.[13] CCIA has concerns about the serious privacy implications created by the Department's proposed regulations to broadly collect, verify, and retain large amounts of data.

---

[9] 50 U.S.C. § 1702(b)(3).
[10] H.R. Conf. Rep. No. 482, 103rd Cong., 2nd Sess., 1994 U.S.C.C.A.N. 398, 483). https://www.congress.gov/congressional-record/103rd-congress/browse-by-date
[11] NPRM, at 5702.
[12] NPRM, at 5727.
[13] *See* Cloudflare, *The Cloudflare Trust Hub* (last accessed April 22, 2024) https://www.cloudflare.com/trust-hub/.

The NPRM invites conflict with compliance requirements and obligations under other privacy regimes. Despite the lack of a comprehensive federal privacy law, there are now sixteen states with a comprehensive consumer privacy law, in addition to countless other sectoral privacy regulations.[14] Businesses must navigate through this growing patchwork of state privacy obligations that often contain restrictions on the collection and storage of personal information. The NPRM is likely to conflict with many of these requirements, complicating U.S. IaaS providers' compliance with applicable regulations. Companies operating in the European Union would face additional difficulties in being able to collect this information under the General Data Protection Regulation including adherence to data minimization principles.

The NPRM seems to be inconsistent with the Department of Justice's efforts to address the risks regarding access to large quantities of U.S. persons data by countries of concern.[15] The CIP requires a company to collect certain types of information about its customers including that of U.S. persons. However, such information would be considered "sensitive data" under the Justice Department's advance notice of proposed rulemaking. As a result, complying with the CIP requirements increases the risk of companies collecting data that could be targeted and accessed by foreign adversaries and malicious actors—undermining the objectives outlined by the Department of Justice.

The NPRM risks encouraging foreign governments to adopt similarly prescriptive measures that would weaken privacy and security protections globally. Foreign resellers of U.S. IaaS products would also be required to collect and maintain information about their customers and foreign individuals, even if the customers use infrastructure that is located outside of the United States. Some foreign governments may be able to demand access to the personal information collected by U.S. providers and their foreign resellers as required by the proposed CIP. Further, foreign governments could impose similar regulations to directly or indirectly target potentially sensitive customers such as dissidents, journalists, and human rights workers.

CCIA's members appreciate the Department's efforts to address the abuse of these services but reiterate that any approach should not come at the cost of privacy.

B. Efficacy of CIP

[14] On April 17, Nebraska Governor Jim Pillen signed LB 1074 (Nebraska Data Privacy Act) into law.
[15] 89 Fed. Reg. 15780 (March 5, 2024).

The proposed CIP is likely to be ineffective at addressing and deterring the abuse of domestic critical infrastructure by malicious foreign actors for several reasons.

First, malicious actors will be able to easily circumvent verification requirements by using IP spoofing, compromised credentials, or a stolen identity. The NSTAC cautions that a "potential repercussion of KYC rules is that the identity-fraud market would expand to meet attackers' demand for seemingly legitimate user credentials and accounts."[16] Companies would need to spend additional resources and personnel to mitigate against this increased risk of abuse. The CIP also would do nothing to prevent threat actors to conduct sophisticated attacks by leveraging other compromised infrastructure as recently illustrated by the "Volt Typhoon" intrusion.[17]

Second, requiring U.S. IaaS providers to sink resources into costly due diligence requirements will detract from more effective efforts to maintain and improve their security posture. Companies have benefited from a risk-based approach to cybersecurity as it has enabled them to respond to the risks most relevant or pressing to their organization. Companies would need to reallocate and spend a substantial amount of resources to establish a CIP, which restricts their ability to proactively invest in security-enhancing measures.

Lastly, the NPRM imposes substantial compliance costs that will restrict individual's ability to use free, security-improving services. Currently, several IaaS providers offer low to no-cost services such as DDOS protection and universal SSL certificates that have benefited small businesses, civil society organizations, and more. However, IaaS providers will not be able to offer many of these free services due to the costs needed to support the NPRM requirements. Limiting the public's access to these important security services will result in a worse overall cybersecurity environment.

C. CIP Exemption

The NPRM proposes creating a process for the Secretary of Commerce to exempt U.S. IaaS providers and foreign resellers from the CIP requirements—notably, this does not extend to

[16] NSTAC Report, at 23.

[17] James Pearson and Raphael Satter, *What is Volt Typhoon, the Chinese hacking group the FBI warns could deal a 'devastating blow'?* Reuters (April 19, 2024) ("...Volt Typhoon has functioned by taking control of swathes of vulnerable digital devices around the world—such as routers, modems, and even internet-connected security cameras—to hide later, downstream attacks into more sensitive target") https://www.reuters.com/technology/what-is-volt-typhoon-alleged-china-backed-hacking-group-2023-05-25/.

the AI reporting requirements.[18] The provider or reseller must establish that their ADP complies with the various requirements but the ADP exemption process contains serious flaws that threaten businesses' ability to obtain and rely upon it, including that an exemption be freely withdrawn at any time.

To obtain an exemption, the Secretary must find that the provider or reseller's ADP companies meet various requirements, including adhering to security best practices to detect and respond to the abuse of IaaS products. However, The NPRM does not specify a timeline for this process or the Secretary's findings. While the Secretary is provided with a lot of discretion to make this determination, the NPRM does not provide any meaningful guidance on how businesses are to apply for the exemption. The NPRM makes clear that the exemption can be "revoked at any time."[19] The proposed rules do not provide any notice of revocation, an opportunity to appeal the revocation, or a grace period if an exemption is denied. The vague standard and risk of arbitrary grants and denials means many companies will choose to invest in ineffective CIPs, rather than pursuing exemptions and implementing effective abuse prevention mechanisms. It also could weaken the industries' trust and confidence in the regulatory program.

CCIA believes that focusing on the development and advancement of best practices to combat malicious cyber activities would be more effective at achieving the Administration's goals. Leading IaaS providers already implement best practices for detecting and responding to the abuse of their IaaS services such as abuse reporting workflows and blackbox monitoring.

[18] NPRM, at 5730.
[19] *Id.* at 5732.

IV. Conclusion

CCIA appreciates the Department's continuous efforts to work with industry and our members remain committed to working with the U.S. government to address national security threats.

Respectfully submitted,

Alvaro Marañon
Policy Counsel, Privacy and Security
Computer & Communications Industry Association
25 Massachusetts Avenue NW, Suite 300C
Washington, DC 20001
Amaranon@ccianet.org

April 29, 2024