U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

April 29, 2024

Mr. Alan F. Estevez
Under Secretary of Commerce for Industry and Security
U.S. Department of Commerce
1401 Constitution Avenue
Washington, DC 20230

Re: Notice of Proposed Rulemaking, *Taking Additional Steps To address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities* (88 Fed. Reg. 5698, January 29, 2024)

Dear Under Secretary Estevez:

The U.S. Chamber of Commerce ("Chamber") appreciates the opportunity to provide comments on the U.S. Department of Commerce ("Department") Bureau of Industry and Security's ("BIS") notice of proposed rulemaking ("NPRM") for implementing Executive Order ("EO") 13984, *Taking Additional Steps To address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities*.

The Chamber's members include global cloud computing companies, technology and cybersecurity providers, financial services entities, and companies in all industry sectors that rely on cloud services—software, platform, and infrastructure—for business operations. Our members are committed to advancing the national and economic security of the U.S. and invest substantial resources to reduce cyber risk.

We acknowledge the underlying objective of the NPRM to address certain national security concerns by implementing a customer identification requirement on infrastructure as a service ("IaaS") providers and resellers, and we recognize that the program is designed to facilitate law enforcement requests for information, to make it more difficult for foreign entities to use U.S. IaaS products for malicious cyber activities, and to safeguard the national security of the U.S. The Chamber understands that these objectives are important for maintaining a secure and resilient digital economy and are committed to working with policymakers to achieve them. Accordingly, we offer the recommendations, comments, and concerns identified in this letter in a spirit of partnership and engagement.

Chamber members currently invest substantial resources in cybersecurity programs and operations. They leverage various abuse deterrence techniques regardless of whether abuse is carried out by a U.S. person or entity or a foreign person or entity operating in the U.S. or a foreign jurisdiction. Businesses face myriad malicious cyber activity, including nation state-backed advanced persistent threat ("APT") actors seeking to infiltrate critical infrastructure and operational technology systems for intelligence or disruptive purposes, execute ransom attacks against systems or data, steal intellectual property, harvest legitimate credentials, and conduct big game phishing attacks. Today's sophisticated malicious cyberattacks establish new infrastructure rapidly, and often obfuscate their location and identity to conduct illicit campaigns and to stay ahead of law enforcement and cybersecurity investigators. In 2023, according to CrowdStrike, it took an adversary an average of 62 minutes—and the fastest only 2 minutes—to move laterally off an initial compromise to conduct surveillance, escalate privileges, and establish persistence on targets.

At the core of the NPRM is the customer identification program ("CIP"), a proposed tool for deterring abuse of domestic infrastructure. We believe that the CIP is unlikely to be an effective deterrent for malicious actors because it will detract from other, more effective approaches and depends on malicious cyber actors providing truthful information about their identity, nationality, and current location. In practice, illicit actors find it easy to circumvent identity verification processes by falsifying or concealing their identities, making it difficult for IaaS providers, law enforcement, cybersecurity services, and legitimate internet users to identify them. This underscores the need for a robust multi-faceted approach to deterring and preventing abuse that can effectively expose illicit cyber actors.

Effectively countering, deterring, and reducing the risk of the abuse of domestic infrastructure requires an overarching, multi-faceted strategy that leverages the tools, technologies, capabilities, and intelligence of several U.S. Government agencies and various private sector actors. While there has been significant advancement in cybersecurity technologies, including artificial intelligence, that aid network defenders, there is widespread recognition that there is no silver bullet for security and identity management. Public and private sector stakeholders must commit to continuous action and a layered, defense-in-depth approach to address cyber threats.

Findings and Recommendations

Recommendation 1.0: The U.S. Government should revise or rescind EO 13984. The most effective way for the U.S. Government to counter abuse of domestic infrastructure ("ADI") is to organize, codify, incentivize, and implement cybersecurity best practices to detect and mitigate abuse. Know Your Customer ("KYC")

requirements are costly, burdensome (especially to small businesses), and ineffective at reducing abuse of IaaS at scale.

The Chamber urges the Department to consider the findings and recommendations included in the National Security Telecommunications Advisory Committee ("NSTAC") report on *Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors*. A new, risk-based, privacy-conscious approach is required to more effectively counter malicious cyber activity.

- **Recommendation 1.1**: The Office of the National Cyber Director should update the National Cybersecurity Strategy Implementation Plan Strategic Objective 2.4 to include *developing a long-term, multifaceted strategy* to combat the ADI and taking into account: (1) the types of and scale of abuse the U.S. Government is concerned with; (2) the tactics of malicious cyber actors; (3) challenges with current IaaS abuse deterrence programs and information sharing; (4) a review of national-level intelligence collection against ADI; (5) an assessment of global privacy implications and international law; (6) an assessment of policy recommendations effectiveness at reducing ADI; and (7) an assessment of the costs on small businesses.

- **Recommendation 1.2.** The Department should split the rules implementing EO 13984 with those implementing EO 14110, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. These large complex EOs demand separate rulemaking processes and adequate consultation from industry to ensure the rules achieve their goals without undermining U.S. competitiveness.

Recommendation 2.0: The Chamber supports the creation of Abuse of IaaS Products Deterrence Programs ("ADP"). We believe that cybersecurity best practices, vice a customer identification program ("CIP") or KYC requirements, will be more effective at countering abuse of IaaS products and raising levels of cybersecurity best practices across providers. However, we urge the Department to provide additional clarity on cybersecurity best practices, take steps to harmonize with other U.S. Government efforts, and model existing best practices for countering ADI.

- **Recommendation 2.1**: The U.S. Government, working through the National Security Council Cybersecurity Directorate, the Office of the National Cyber Director ("ONCD"), the Cybersecurity and Infrastructure Security Agency ("CISA"), the National Institute of Standards and Technology ("NIST"), the Department of Justice, and other federal agencies as appropriate and in consultation with industry stakeholders, should develop cybersecurity best practices for an effective ADP.

- **Recommendation 2.2**: Cybersecurity best practices in the ADP should consider and align with technologies mandated for federal agencies and contracts in EO 14028, *Improving the Nation's Cybersecurity*, to include endpoint detection and response, zero trust architecture, and log management. These technologies should be voluntarily applied to the unique IaaS products and appropriate to the risk.

Recommendation 3.0: The Department should eliminate or take steps to significantly narrow the CIP requirement. The U.S. Government has suggested that a requirement for U.S. IaaS providers to implement a CIP or KYC program would prevent or reduce malicious cyber activity. However, malicious threat actors are more commonly using temporary infrastructure such as virtual private network tunnels, voice-over-internet protocol ("VOIP") telephone numbers, pre-paid credit cards, pay-as-you-go cloud storage systems, and compute nodes to effectively obfuscate their illicit activity across a wide range of technology and providers. Even when detection is possible, malicious actors move quickly, dismantling or abandoning infrastructure.

- **Finding 3.1:** The U.S. Government should not compare KYC requirements in the financial services sector to those proposed for U.S. IaaS providers. The financial services sector cooperates globally through a variety of international agreements and policymaking bodies that have facilitated the creation of global, industry-wide standards and processes for identity verification. No such global cooperation or international standards exist in the IaaS industry and foreign IaaS providers generally do not implement identity verification. The Chamber is not aware of any academic, government, or industry analysis comparing KYC requirements across the sector.

- **Finding 3.2:** CIP is unlikely to effectively address malicious cyber activity. Malicious cyber actor, especially those advanced persistent threat actors associated with The People's Republic of China, the Islamic Republic of Iran, the Democratic People's Republic of Korea, and the Russian Federation are most likely to use tactics, techniques, technologies, and methods to bypass cybersecurity controls, obfuscate their name and location, and avoid detection by compromising legitimate credentials thereby appearing to be a U.S. person. Identity attacks, access brokers, and prolific abuse of valid credentials have increased significantly in the last few years. By using legitimate credentials to establish legitimate access to achieve persistence and lateral movement, malicious actors avoid detection from network defenders.

- **Finding 3.3:** KYC requirements will likely impact businesses' obligation to international privacy rules and the U.S. Government's privacy priorities. The

Chamber members operate in numerous domestic and international jurisdictions, each with their own set of statutes, regulations, and commercial agreements governing how companies collect, process, store, and transfer customer data. While the European Union's ("EU") General Data Protection Regulation ("GDPR") is often the most commonly known, many of these laws typically apply to information used to identify a person (*e.g.*, name, address, date of birth), but also may take on a more expansive definition of identifiable personal data, such as email addresses, IP addresses, employee username and email, employee user IP logs, MAC addresses, cookie IDs, and other employee device identifiers. Businesses must evaluate each jurisdiction's privacy and data requirements with an eye toward compliance within an increasingly disparate and complex regulatory landscape. For businesses, non-compliance risk could result in market access loss, financial sanctions or penalties, reputational harm, or legal liability.

Since the Court of European Justice invalidated the U.S.-EU Privacy Shield in the Schrems II case, European privacy regulators have scrutinized U.S. cloud service providers' processing of EU citizen data due to concerns about the ability of U.S. Government agencies to access such data. In addition, European Commission officials and EU Member State governments have routinely and regularly criticized the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act"), which provides a legal process for U.S. cloud service providers to produce data even if that data is located outside of the U.S. to U.S. law enforcement.

In response to businesses' concerns regarding transatlantic data flows and European data privacy concerns, the U.S. Government issued EO 14086, *Enhancing Safeguards for U.S. Signals Intelligence Activities*, which updated and enhanced privacy and civil liberty safeguards across eighteen U.S. intelligence agencies. This resulted in the U.S. and European Commission renegotiating the Transatlantic Data Privacy Framework, which enables transatlantic data flows.

The Chamber emphasizes how vital the transatlantic data flows are to its members. Similarly, we note that privacy-enhancing measures are of critical importance to European regulators. Any U.S. Government tools that appear to provide new surveillance or government access to EU citizen's data could create doubt about the U.S. Government's commitment to data privacy and trigger a response from the EU that negatively impacts the businesses that are of vital importance to American economic and national security. Accordingly, we urge the U.S. Government to engage in robust digital diplomacy to ensure that this potential outcome is averted.

- **Finding 3.4:** The CIP and KYC requirements will inhibit U.S. IaaS competitiveness and advantage cloud service providers from foreign adversary nations. The U.S. Government, including the Department of Homeland Security and Department of State have been on the forefront of dealing with efforts by foreign jurisdictions to impose digital sovereignty requirements—in violation of WTO trade rules—that discriminate against U.S. cloud services providers. The privacy concerns outlined in Finding 3.3 above will advantage digital sovereignty supporters and disadvantage free flows of data critical to the modern global economy.

  The Chamber also is concerned with Chinese cloud services providers undermining secure and trusted vendors in emerging markets by selling below cost to capture market share. We urge the U.S. Government to incentivize digital transformation through the promotion of secure and trusted cloud services. Ukraine's use of U.S. cloud services is a success of secure and reliable digital infrastructure stands in contrast to the case of the African Union where sensitive data was routed from Huawei-installed servers back Shanghai (See Heritage Foundation, *How China Has Been Using Huawei-Made Cameras to Spy on the African Union Headquarters* and U.S. Department of State, *How the People's Republic of China Seeks to Reshape the Global Information Environment*).

Recommendation 4.0: The Department should consider the impact of a burdensome and costly CIP, particularly on small businesses.

- **Finding 4.1:** Management of CIP and KYC requirements will be resource intensive and cost prohibitive, particularly for new market entrants and small businesses. While small IaaS providers are making investments in cybersecurity and abuse mitigation measures, they face significant resource challenges. Due to cost limitations, these providers often lack the resources to implement advanced protections such as tools to prevent account compromise, fraud, and log analysis.

  Additionally, small businesses may be negatively incentivized to proactively identify and address malicious activity on their platforms due to legal and reputational concerns. Sharing threat information with other companies or the government can increase liability risks and trigger privacy-related constraints that create disincentives for threat-hunting operations and information sharing. Small and mid-sized businesses may also struggle to access commercially available tools for detecting cyber threats, either due to cost considerations or

gaps in human capital skills to implement, design, and manage complex cybersecurity services.

Adding a requirement that IaaS providers implement a CIP, on top of other abuse prevention mechanisms, will impose significant resource burdens, particularly on small IaaS providers, and divert resources away from effective efforts to deter abuse. Implementing a CIP will require providers to set up entirely new compliance teams to develop, implement, and maintain a compliant CIP. Financial institutions have entire teams devoted to identity verification and expend considerable resources on their programs. Requiring similar efforts across the entire U.S. IaaS industry will impose significant costs on providers, while doing little to address malicious cyber-enabled abuse.

The challenges small IaaS providers face demonstrate their unique needs and limitations in enhancing their cybersecurity measures and navigating the complex legal and regulatory landscape. Therefore, it is imperative that more support is provided to small businesses to promote information sharing, combat infrastructure abuse, and enhance their cybersecurity measures effectively.

- Recommendation 4.2: The Department should eliminate the CIP requirement and focus resources on developing and implementing best practices to deter abuse, as discussed above. If the Department imposes a CIP requirement, however, it should implement a tiered approach for IaaS size, complexity, products, and risk profile. To ensure a uniform and standardized approach to potential covered entities, the Chamber recommends use of the Census Bureau's North American Industry Classification System (NAICS) to establish a methodology for fair and balanced implementation of new regulations that will ensure that smaller entities are not disproportionately burdened.

Recommendation 5.0: The Department should modify CIP exemptions and processes.

- Recommendation 5.1: The Department should establish a clear timeline and procedure for ADP exemption decisions and limit the Secretary's discretion to deny or revoke an exemption. The Chamber supports the security best practices and outcome focus of the ADP. To provide certainty to industry and allow IaaS providers to rely on the exemption process, however, the Department should provide additional clarity around the ADP decision timeline and requirements and limit discretion to deny or revoke an exemption. Considering the extremely high cost, burden, and legal analysis required to implement a CIP, the Chamber recommends that the Department provide clarity that an entity submitting a request for an exemption from CIP requirements does not need to develop a

CIP while the Secretary of Commerce reviews its application. In the event of either an exemption approval or denial, we recommend the Department provide a period of at least two years for an entity to implement a CIP. The Chamber believes that businesses should be allowed to deploy their finite cybersecurity resources on risk management and implementing the cybersecurity best practices of an ADP. While it is possible that an IaaS provider could concurrently implement both an ADP and CIP while awaiting a decision on an ADP exemption, we question whether the best use of resources would be the establishment of both programs and could envision small businesses being especially challenged with the costs of implementing both programs. For these reasons, we recommend that the Department provide clarity for IaaS providers regarding their responsibilities for implementing an CIP while awaiting an ADP exemption decision.

- Recommendation 5.2: The Department should strengthen investment in security best practices and the implementation of an ADP by providing a clear path to meeting the security expectations of the Department. To do this, the Department should work with industry to develop abuse prevention best practices that could form the basis of the ADP and provide that providers will receive an exemption if they implement an ADP consistent with these best practices. The Department also could use the ADP to provide a continuous feedback loop such that improvements can be made as new cybersecurity technologies and privacy-preserving tools enter the market, reflecting a new threat environment. The Department should not add financial liability to IaaS providers pursuing security best practices but incentivize them to implement a robust ADP by creating clear risk-informed benchmarks for a provider to meet. In the case of an ADP denial, the Department should provide a written explanation of an ADP denial and create an appeals process to adjudicate challenges to decisions. The provider should not be required to implement a CIP until the appeals process is complete.

- Recommendation 5.3: The Department should clarify criteria for the revocation and establish a process for dispute resolution and adjudication. The Chamber expects that U.S. IaaS providers will invest significant resources into the establishment and compliance with an ADP. Accordingly, we urge the Department to increase confidence that ADP investments will be safe from arbitrary revocation by providing additional clarity on the criteria by which an ADP will be revoked. Further, the Department should provide clarity that an ADP will not be removed at any time without recourse. U.S. IaaS providers who have been determined by the Secretary of Commerce to have an adequate ADP and have been granted an exemption from the CIP should be provided in writing a full, evidenced-based determined on the failure of the ADP to identify,

detect, or respond to red flags and provided an opportunity to enhance its cybersecurity best practices to bring the ADP back into compliance with the Department's security expectations before being required to implement a CIP.

- Recommendation 5.4. The U.S. Government should limit the CIP requirement to foreign customers from countries of concern, or, at a minimum, exempt from the requirement customers from countries with significant security (*e.g.*, The Five Eyes, NATO Treaty Allies, Quadrilateral Security Dialogue countries) and trade partnerships (e.g., United States-Mexico-Canada Agreement, Free Trade Agreement countries) with the U.S., adhering to World Trade Organization ("WTO") principles. In consideration of any exemption the U.S. Government should consider whether a foreign jurisdiction has a mutual legal assistance agreement with the U.S. or is a signatory to the Budapest Convention on Cybercrime. The Chamber views the NPRM's CIP requirements as both a threat to U.S. IaaS providers' ability to compete globally, specifically in the EU, and a threat to ongoing negotiations with the EU on free flows of data.

  The Chamber is a longtime advocate for strong commercial ties between the U.S. and the EU and is a leading business voice on digital economic policy. In the U.S., Europe, and globally, we advocate for sound policy frameworks that support economic growth, promote data protection, and foster innovation. Many of the Chamber's members are heavily invested in the EU, which is collectively the largest primary U.S. export market. The Chamber applauded the European Commission's July 2023 adequacy decision for the EU-US Data Privacy Framework, which allows personal data to flow freely between U.S. and EU companies. Transatlantic data flows are vital to the bilateral business relationship.

  The Chamber is concerned that the rules implementing EO 13984 will jeopardize U.S. IaaS providers' global competitiveness, especially in the European cloud marketplace. Since January 2021, the Chamber has conveyed that KYC requirements will negatively affect the ability of U.S. IaaS providers to compete in the EU at a time that when European member states are actively supporting policies and programs that are likely to exclude U.S. cloud service providers from the digital single market (*e.g.*, GAIA X initiative, French SecNumCloud, EU cloud security scheme, the future Cloud Rulebook). This EO could further undermine U.S. competitiveness in the EU marketplace.

  Several EU Members States have concerns with the alleged collection of EU-persons information by U.S. Government entities and have promoted a digital sovereignty agenda through EU institutions in response. The draft candidate scheme for the cybersecurity certification of cloud services ("EUCS") is an

example of a policy initiative meant to address the protection of European data against concerns of unlawful access. Iterations of the draft scheme have included requirements for non-EU cloud computing companies to localize and process data in the EU. The Chamber is concerned that the KYC / CIP rules implementing EO 13984 will drive EU member states to advance the EUCS with localization requirements, which would negatively impact global commercial flows and exclude trusted American cloud service providers from the European market.

Hard data localization requirements are profoundly negative for global cybersecurity. According to an academic paper titled *The Effects of Data Localization on Cybersecurity - Organizational Effects*, not only would the availability of cyber threat telemetry and intelligence be significantly reduced for cyber defense, but implementing effective cybersecurity controls like International Standards Organization ("ISO") controls would be negatively affected as well.

- **Recommendation 5.5:** The Department should confirm that the definition of IaaS products is not meant to include blockchain networks and blockchain sequencers. Simply applying the rules to these networks will not achieve the government's goals. Blockchain networks are unique in the sense that they can only be attacked by controlling many of the validators on the network, which is prohibitively expensive and has never been done for the largest networks. Additionally, to the Chamber's knowledge, blockchain networks have never been used as vectors to attack U.S. persons or entities. The blockchain code is open and visible to anyone, which means that cybersecurity threats within the blockchain itself would be visible to everyone.

  Transactions on blockchain networks with sanctioned persons or entities are already subject to prohibitions, and application providers on blockchain networks have existing anti-money laundering or KYC programs. However, implementing the NPRM's KYC program on blockchain networks is not feasible since these networks are run on open-source software, which can be developed and built upon without permission by anyone. There is no central entity to implement the KYC program or collect the relevant information. Blockchain sequencers, being an additional network layer built on top of other blockchain networks, should be covered by any exemptions given the broad scope of the definitions in this proposal. For the Department to achieve its goals, it should create an exemption for decentralized, public, permissionless blockchain networks and blockchain sequencers.

Recommendation 6: The Department should modify the reporting requirement on large AI models to address legal, technical, and policy defects. Likewise, the Administration should reconsider the NPRM's large AI model reporting requirements to address several significant legal, technical, and policy shortcomings that will undermine its effectiveness. As a legal matter, the Administration must explain how the large AI model reporting requirements can be squared with the Stored Communications Act, which explicitly prohibits electronic communications services and remote computing services from disclosing customer records absent lawful process, the consent of the customer, or in narrowly defined circumstances that do not appear applicable here. Unless the Department provides reasonable assurances about the lawful basis for compelling such information, IaaS providers will encounter tremendous legal uncertainty as they seek to navigate compliance with the large AI model reporting requirement and the Stored Communications Act. The reporting requirement is also technically flawed. It requires IaaS providers to report on customer information – *e.g.*, "AI training practices" and "cybersecurity practices" – to which they do not have direct access. The definitions of "training," "training run," and "large AI model" are also overly broad, potentially sweeping in a broad swath of models that pose limited risks. The reporting requirement will ultimately undermine U.S. national security by undermining trust in American IaaS providers, alienating allies, and driving international customers to less secure cloud service alternatives offered by foreign companies that are not subject to similar reporting requirements.

- **Recommendation 6.1:** To narrow the scope of the rule and allow for more targeted reporting, we urge the Department to clarify that the rule is not intended to capture fine-tuning.

  The Department should issue guidance with specific, narrow technical criteria for when a model meets the large model definition and is subject to reporting. These criteria should limit reporting to when a foreign customer is using:

  1) A specific amount of compute capacity (*e.g.*, 10^26 floating-point operations);
  2) Derived from integrated circuits that are subject to the Export Administration Regulations and classified as Export Control Classification Numbers 3A090.a; and
  3) Within a limited period of time (*e.g.*, 3 months) to train a model.

  These are the appropriate criteria for controls because they are the only criteria into which a provider normally will have visibility. Usage of compute capacity must be constrained to a limited time period because otherwise the requirement will capture customers who cross the compute threshold after using compute power for an extended period of time for purposes other than

training. Providers should be required to report only the amount of compute and type of infrastructure the customer is using for training, rather than detailed, sensitive information on training and cybersecurity practices.

- **Recommendation 6.2**: The Department should limit the scope of the reporting requirement to foreign customers based in specific countries of concern.

###

We look forward to engaging with the Department and the broader Administration to strengthen our collective defense and counter abuse of domestic infrastructure in a risk-based, privacy-enhancing manner.

Sincerely,

Vincent M. Voci
Vice President, Cyber Policy and Operations
Cyber, Space, and National Security Division
U.S. Chamber of Commerce

Christopher D. Roberti
Senior Vice President
Cyber, Space, and National Security Division
U.S. Chamber of Commerce