April 29, 2024

Via Electronic Submission

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

RE: E.O. 13984/E.O. 14110: NPRM

The Software & Information Industry Association ("SIIA") appreciates the opportunity to provide these comments in response to the Bureau of Industry and Security ("BIS") request for comment ("RFC") on the Notice of Proposed Rulemaking ("NPRM") (Docket No. 240119-0020/RIN: 0694-AJ35).

SIIA is the principal trade association for companies in the business of information. Our nearly 400 members include cloud service providers, companies reflecting the broad and diverse landscape of digital content providers and users in academic publishing, education technology, financial services, creators of software, as well as platforms used by billions of people worldwide.

The NPRM[1] aims to implement two separate executive orders: Executive Order 13984 of January 19. 2021, on *Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities* (hereafter referred to as the "IaaS EO")[2], and Executive Order 14110 of October 30, 2023, on the *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (hereafter referred to as the "AI EO")[3].

In its request for comment, BIS states that the proposed rule seeks to advance a three-fold purpose: (1) require U.S. Infrastructure as a Service ("IaaS") providers to implement programs to maintain records related to IaaS accounts where foreign persons have an interest and to verify the identity of such persons; (2) prevent foreign persons from using U.S. IaaS products to conduct malicious cyber-enabled activities; and (3) safeguard U.S. national security.

SIIA strongly supports the Administration's efforts to combat malicious cyber-enabled activities. Our members partner with the Department of Commerce ("Department") and other relevant U.S. government agencies and are committed to doing their utmost to address national and cybersecurity threats, including those related to the training and deployment of large AI models. Yet we are concerned that the NRPM, as written, fails to adequately address the concerns that underpin both the IaaS EO and the AI EO; that it will negatively impact the competitiveness of U.S. cloud service providers abroad; and,

[1] 89 FR 5698.
[2] The IaaS EO is available at https://www.federalregister.gov/documents/2021/01/25/2021-01714/taking-additional-steps-to-address-the-national-emergency-with-respect-to-significant-malicious
[3] The AI EO is available at https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence

that it likely will undermine important U.S. government efforts related to privacy, the international transfer of data, and even the national security objectives set out in the NPRM.

1. Background

The last two presidential administrations have identified a growing threat from foreign malicious cyber actors, who leverage U.S. IaaS products and services to commit intellectual property and sensitive data theft, engage in covert espionage, and threaten U.S. critical infrastructure.[4]

In an effort to address these concerns, President Trump issued the IaaS EO to direct the Secretary of the Commerce ("Secretary") to propose regulations that would require U.S. IaaS providers to verify the identity of their foreign account holders[5] – referred to in the NPRM as a Customer Identification Program ("CIP")—as well as, under certain circumstances, prohibit or place conditions on foreign persons' use of U.S. IaaS services.[6] The Department published an advanced notice of proposed rulemaking soliciting to implement provisions of the IaaS EO.

President Biden issued the AI EO prior to issuance of the pending NPRM. Section 4.2(c) of the AI EO directs the Secretary to propose near identical obligation on foreign resellers of U.S. IaaS products and services.[7]

In accordance with the IaaS EO, the NPRM also envisions authorizing the Secretary to, if necessary, impose so-called special measures to require U.S. IaaS providers to prohibit or limit access to accounts that foreign actors use to conduct malicious cyber-enabled activities.[8] Finally, the NRPM proposes to allow the Secretary to exempt any IaaS provider from the aforementioned requirements, including in situations where the provider complies with established best practices to deter abuse.

In sum, the NPRM seeks to impose a raft of obligations on U.S. IaaS providers. These include implementing and maintaining a written CIP that requires all U.S. IaaS providers and all of their foreign resellers of U.S. IaaS products to obtain information that verifies the identity of any potential foreign customer or foreign beneficial owner prior to the opening of an account; ensure that all foreign resellers comply with CIP requirements; and to terminate any reseller relationship within 30 days if the reseller is out of compliance.[9] In addition, the NPRM includes a number of reporting requirements related to transactions that either result in, or could result in, the training of a large AI model with potential capabilities that could be used in malicious cyber-related activity.[10]

---

[4] *Supra* note 1.
[5] *Supra* note 2 §1(a).
[6] Id. §2(d)(i) and (ii).
[7] *Supra* note 3 §4.2(c)(ii).
[8] *Supra* note 1.
[9] Id. §7.302.
[10] Id. §7.308.

2. The Proposed Regulations are Inconsistent with the Stored Communications Act

As an initial matter, the NPRM appears to suffer from at least two legal infirmities that BIS will need to either remedy or adequately explain before a final rule can be promulgated.

The Stored Communications Act[11] ("SCA") prohibits a remote computing service from disclosing customer communications or records without lawful process unless an exception applies. Some information required by the proposed rule related to AI training runs, such as the name of the foreign customer, its address, telephone number, and means and source of payment[12] constitutes basic subscriber information ("BSI") under the SCA, and none of the exceptions are relevant.[13] The government can only obtain this data pursuant to legal process.

In addition, the proposed rule would require U.S. IaaS providers to engage in an ongoing and/or prospective logging of foreign customer information (i.e., IP address collection). Doing so would require American companies to "install or use a pen register or a trap and trace device," which, absent a court order, is illegal.[14]

An executive order or administrative rule cannot preempt or supplant a statute. And it goes without saying that any final rule, at a minimum, must be clear that U.S. IaaS providers only can be required to disclose BSI pursuant to the legal process requirements in the SCA, and that they are not, under any circumstances, compelled to engage in otherwise illegal conduct, such as using a pen register or similar to record non-BSI foreign customer information.

3. Overly Broad and Ambiguous Definitions Will Undermine Government Objectives

We are concerned that the breadth and ambiguity of key terms in the proposed regulations will lead to uncertainty and increase the risk of non-compliance. A few examples can serve to illustrate.

One notable example is the proposed definition of a "Large AI model with potential capabilities that could be used in malicious cyber-enabled activity," which is both vague and overbroad. Among other things, it includes "*any* AI model with the technical conditions of a dual-use foundation model *or otherwise has technical parameters of concern* that has capabilities that *could be used to aid or automate aspects* of malicious cyber-enabled activity [if] *it meets the technical conditions described in* [subsequently issued] *interpretative rules* […]."[15]

We have previously addressed concerns about how the definition of "dual-use foundation model" is difficult to implement as it is and can lead to a slippery slope.[16] The proposed definition

[11] 18 U.S.C. 121 §2701 *et seq*.
[12] *Supra* note 1 §7.308(d).
[13] *Supra* note 11.
[14] 18 U.S.C. 206 §3121.
[15] *Supra* note 1 §7.301. (emphasis added)
[16] See SIIA's response to NTIA's Request for Comment regarding *Dual Use Foundation Artificial Intelligence Models with Widely Available Model Weights* at 2-3. The comment is available at https://www.siia.net/siias-response-to-ntias-request-for-comment-regarding-dual-use-foundation-artificial-intelligence-models-with-widely-availablqe-model-weights/

explicitly covers a broader universe of AI models. While we understand the interest in cutting off potentially malicious tools at their source, U.S. IaaS providers do not have visibility into their customer's models, including their capabilities or training practices. The only criteria related to a customer's model into which a provider will normally have visibility is the amount of compute capacity and type of infrastructure that the customer is using. It is also very unlikely that the customer will be willing to provide this information to the IaaS provider, as it is considered extremely sensitive and confidential.

It is also not possible for U.S. IaaS providers to anticipate how AI models will be used. The breadth and numerous ambiguities in the definition could be read to require providers to comply with the recordkeeping and reporting requirements under the proposed rule for any AI model training by a foreign person. It is therefore imperative that BIS clarify in the regulations that a model will meet the large AI model definition and be subject to reporting only if it meets specific technical criteria into which the IaaS provider has visibility, and that is narrowly tailored to target the large, dual-use foundation models that are of concern to the government.

Similarly, the proposed definition of "training" or "training run" as "any process by which an AI model learns from data using computing power"[17] will lead U.S. IaaS providers to demand recordkeeping information from virtually all foreign customers. The definition also does not distinguish between pre- and post-training and provides no threshold for what constitutes a "large" training run. In addition, it is unclear if the contemplated definition of a training run might include the process of fine-tuning models. If that is the case, the potential scope of the rule will become enormous. BIS should clarify that the proposed regulations do not cover fine-tuning of a model.

Also, the proposed definition of a "covered transaction" related to large AI model training goes beyond formal transactions to include "*any usage* of services by, for, or on behalf of a foreign person *that results or could result* in the training of a model with the capabilities that could be used in malicious cyber-enabled activity" described in earlier sections of the proposal.[18]

A definition this broad means that a U.S. IaaS provider would need to conduct diligence on and demand customer information from virtually any customer that purchases compute capacity—because almost any purchase of compute *could* result, at some point, in the customer training a large AI model—as well as nearly anyone who may conceivably use the IaaS services in connection with a customer account. To address this, BIS should clarify the definition of "covered transaction" to include only "usage of services by a foreign person that results in the training of a large model…" and issue narrow technical criteria targeting large dual-use foundation models, as recommended above.

In addition to uncertainty and a risk of non-compliance, we have concerns that these broad ambiguous definitions will undermine the national security objectives of the executive orders. Among other things, the definitional framework will lead U.S. IaaS providers to devote resources across a broader landscape rather than in a targeted manner better designed to identify potentially malicious actors. Likewise, requiring U.S. IaaS providers to collect, maintain, and report to the government mounds of data that have no, or only limited, relevance to the purpose of the proposed rule runs the risk of overwhelming BIS enforcement efforts, thereby limiting its ability to focus on the AI models and

[17] *Supra* note 1.
[18] Id. §7.308(b). (emphasis added)

foreign malicious actors that raise legitimate national security concerns. It also will raise significant privacy and security concerns for foreign customers, who will not want to provide U.S. IaaS providers with sensitive and confidential information on their activities, and could result in foreign customers moving their workloads to foreign IaaS providers or less secure on-premises infrastructure.

Finally, it is also problematic that the NPRM seeks to implement different executive orders through one rulemaking process, despite the fact that the regulations implementing these executive orders are at different stages of ripeness. The part of the proposed rule that is based on the IaaS EO has been subject to extensive engagement between the U.S. government and industry, as well as a formal government-sanctioned study, *infra*, whereas the thinking around implementation of the AI EO is significantly less developed. Because of this, the AI EO would benefit from additional and thorough industry and stakeholder engagement to better understand the risks associated with AI training runs, including indications of malicious activity, and how best to identify them before proceeding to write implementing regulations. It would, therefore, be advisable for BIS to separate the two executive orders and implement them through different regulations.

4. It Will be Easy for Malicious Actors to Evade the Proposed Rule's CIP Requirement

As mentioned, the NPRM is based on the notion, first introduced in the IaaS EO, that requiring U.S. IaaS providers to create a CIP and mandating the collection of various identifying information about their foreign customers will deter foreign malicious cyber actors. There are, however, numerous reasons to doubt the effectiveness of this approach, not least because it will be easy for a determined actor to evade. Establishing a novel customer identification regime without the domestic and international legal and regulatory frameworks that govern the reporting of suspicious financial transactions and anti-money laundering detection in the global banking system, for example, will most likely lead malicious actors to find workarounds.

First, it would be quite simple for malicious cyber actors to sidestep these measures by using false identities and credentials, or transacting with third parties that effectively mask the beneficial owners' IaaS accounts. Incidentally, it is not inconceivable that this also could end up exposing more people to the threat of identity theft.

Second, the use by malicious cyber actors of false identities likely also would make it harder for BIS and other enforcement agencies to investigate specific cyber-attacks and more difficult to identify the individuals and/or groups who are behind them.

Third, the CIP requirements will almost certainly incentivize foreign malicious cyber actors to use non-U.S. IaaS providers, which would not be subject to the proposed rule, thereby undermining or limiting the ability of the U.S. government to effectively combat the type of cyber incidents that the NPRM seeks to prevent. Foreign IaaS providers may not ascribe to the same overall approach to cybersecurity and privacy that U.S.-based IaaS providers support. Moreover, they may have less experience detecting and taking active steps to address malicious cyber activities. This includes proactive engagement with the U.S. government and responsiveness to U.S. government inquiries relating to malicious and criminal activity. There is little doubt that this would have negative implications for U.S. national security and cybersecurity deterrence efforts around the world.

5. Compliance Will be Onerous, Especially for Small- and Medium-Sized Businesses

Notwithstanding the serious legal concerns associated with the NRPM raised in Section 1, *supra*, complying with the proposed rule would be onerous and costly, particularly for small- and medium-sized companies.

First, because the NPRM seeks to impose a set of new reporting requirements for AI training runs, existing contracts between U.S. IaaS providers and their foreign customers or resellers are unlikely to account for the proposed changes. Because of that, customer contracts would almost certainly need to be renegotiated. Even assuming that the customer would accept all of a sudden having to divulge additional information, much of which likely would be considered proprietary and business sensitive, renewing these contracts would temporarily disrupt business operations between the parties.

Second, many foreign customers would likely be reluctant to share the type of information on their AI model training practices that the proposed rule would require, given its business sensitive and confidential nature. And since "foreign person" is defined broadly and not limited to actors that are thought to present a national security risk, the obligation would put the U.S. IaaS provider in an almost impossible position. On the one hand, the provider would be obligated to collect and submit to the U.S. government information that its foreign customer, on the other, would be unlikely to willingly provide.

Third, the CIP requirement would impose on U.S. IaaS providers a substantial additional resource burden, irrespective of whether the activities of the foreign customer raise any reasonable national security concerns or not. Providers will be required to stand up entirely new compliance teams to develop, implement, and maintain a compliant CIP, which will require significant expenditure of time and resources. The U.S. banking industry, for example, spent $25 billion, or approximately 5.2 percent of the industry's revenue that year, implementing "know-your-customer" compliance in 2019.[19]

Applying that benchmark to the U.S. IaaS industry's revenue of $48.6 billion[20] indicates that a CIP could cost $2.5 billion annually, which is significantly higher than the cost estimated by BIS in the NRPM. These additional cost and compliance burdens will be particularly acute for small- and medium-sized companies, which are more resource-strapped and less likely to have in place large in-house legal, policy and/or compliance teams that can help them navigate new and complicated regulations. It may also detract from other cybersecurity efforts that would be helpful in mitigating malicious activity.

Fourth, it is worth pointing out that the NPRM seeks to impose these obligations only on U.S. IaaS providers. Given that the products and services that are at issue here are global in nature, which means that foreign actors—not only malicious actors, but also legitimate business entities that wish to avoid cumbersome and invasive domestic U.S. regulatory requirements—easily can move their workloads to non-U.S. providers. Forcing these types of identity verification and reporting requirements

[19] See KPMG Insights, *Combating Financial Crime*. Available at https://kpmg.com/mc/en/home/insights/2019/03/combating-financial-crime-fs.html; Statista, *Banking Revenue in the U.S. 2010-2022*. Available at https://www.statista.com/forecasts/409713/banking-revenue-in-the-us

[20] Statista, *Infrastructure as a Service – United States*. Available at https://www.statista.com/outlook/tmo/public-cloud/infrastructure-as-a-service/united-states

only on U.S. companies, therefore, will almost certainly put them at a disadvantage vis-à-vis their foreign competitors, which will hurt those companies as well as U.S. economic interests.

Fifth, the AI reporting requirements in the NPRM seek to impose on U.S. IaaS providers an obligation that, as a practical matter, is almost impossible for them to meet. Simply put, IaaS providers do not have information about their customer's "AI training practices" or "cybersecurity practices." Requiring them to obtain this information would be at odds with the IaaS business model, which likely would result in a loss of business for U.S. IaaS providers and undermine U.S. competitiveness abroad.

Finally, the proposed rules may go beyond what data protection rules in foreign jurisdictions authorize. Where there is no means for a U.S. IaaS provider to compel a foreign person to provide the information that the regulations demand, foreign persons will inevitably opt for non-U.S. providers, which may undermine U.S. interests in advancing a digital ecosystem that meets baseline privacy and security protections.

6. The Proposed Regulations Will Destabilize International Data Flows

In addition, the effect of the proposed reporting requirements could have both legal and practical ramifications that reach well beyond the United States, by undermining U.S. government efforts on other fronts, including those related to privacy and international data flows.

As BIS is surely aware, the Department was instrumental in recently reaching an agreement with the European Union ("EU") on the EU-U.S. Data Privacy Framework ("DPF"). The DPF, and the European Commission's subsequent adequacy decision pertaining to privacy protections afforded EU residents under U.S. law, became necessary for U.S. and EU headquartered companies to fully resume transatlantic data transfers after the European Court of Justice invalidated its predecessor EU-U.S. Privacy Shield mechanism in *Schrems II*.[21]

Any actions undertaken by the U.S. government that could undermine global confidence in the privacy protections available to foreign nationals, including through the promulgation of regulations such as the NPRM, would likely raise serious doubts about the future of the DPF and the European Commission's adequacy decision, as well as other such agreements to which the United States is a party. This concern is compounded because the proposed AI reporting regulations would seemingly go beyond the restrictions on government access to information set out in the SCA.

We are also concerned that the NPRM fails to adequately grapple with the presumed effectiveness of the proposed new measures, including untested CIP procedures, relative to the likely negative competitive impact that those requirements will have on U.S. IaaS providers and U.S. global tech leadership more broadly. The global cloud services market is fast-paced and highly competitive, and a proper accounting of how the proposed rule would impact U.S. companies and their ability to maintain current and future business relationships with legitimate foreign customers is therefore essential.

[21] Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems*, ECLI:EU:C:2020:559 (July 16, 2020). The case involved a complaint from an Austrian citizen, who claimed that Facebook's transfer of his data from its Irish subsidiary to its servers in the U.S. was illegal because U.S. law failed to adequately protect his personal data. The European Court of Justice agreed and invalidated the EU-U.S. Privacy Shield framework.

7. A More Constructive Way Forward

As mentioned earlier, while there may be situations where it could make sense to combine multiple regulatory workstreams into one rulemaking, that is not the case here. The proposed rule to implement the IaaS EO is supported by a well-developed record based on constructive and lengthy exchanges between BIS and stakeholders, as well as the thorough work of a presidential commission. There has been no similar effort to understand the practical effects and potentially serious unintended consequences of the AI EO. Because of that, we strongly recommend that BIS split the two EOs into separate rulemakings.

One of the foundational elements of the proposed rule is that it will require that "all U.S. IaaS providers implement their own CIPs, require CIPs of their foreign resellers, and report to the Department on these CIPs."[22] As alluded to earlier, however, it is by no means clear that this approach, which will impose a substantial burden on all U.S. IaaS providers, will live up to its intended purpose.

To the best of our knowledge, there are currently no major IaaS providers anywhere that use anything like the CIP procedures that the NRPM envisions. What we do know is that the CIP, or "know-your-customer" requirements, that are described in the IaaS EO have been the subject of a substantial study commissioned by the President, and that the resulting report found that it was, at best, unclear if the proposed requirements would be useful.[23] Some of the reasons why CIPs are unlikely to be effective have been described earlier in the comment and include that sophisticated malicious cyber actors rarely use their own identifying information to open accounts, and that they change their tactics, techniques, and practices in response to new regulatory requirements.[24]

In addition, there seems to be some confusion about how similar the requirements that the NPRM proposes are to "know-your-customer" measures that currently apply to the financial services sector. But there are, in fact, key differences. The process involved in opening a bank account is vastly different from opening an IaaS account, and the fast-evolving nature of the IaaS industry compared to the banking industry also militates against making any easy comparisons between the two.[25] Moreover, financial institutions cooperate globally on identity verification through an array of international agreements and policymaking bodies, none of which exist in the IaaS industry.

Finally, it bears repeating that an obligation for U.S. IaaS providers to collect and retain the personal information of their foreign customers as part of a CIP would have substantial privacy implications that likely would be at odds with international obligations undertaken by the U.S. government, including the recently agreed DPF, and therefore could further the push for increased digital sovereignty in other parts of the world.

---

[22] *Supra* note 1 at 5703.

[23] The President's National Security Telecommunications Advisory Committee ("NSTAC"), NSTAC Report to the President, *Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors*, September 26, 2023. The report is available at 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

[24] Id. at 23.

[25] Id.

Instead of a CIP, whose effectiveness in wholly unproven, we recommend that BIS center the proposed rule on the Abuse of IaaS Products Deterrence Program for IaaS Providers ("ADP") that is noted as an exemption in the proposed regulation.[26] Specifically, BIS should work with relevant U.S. government agencies and with industry to develop best practices for abuse prevention and require adoption of those best practices, rather than a CIP. Such an anti-abuse program, that focuses on developing and implementing cybersecurity best practices, will provide a more effective way to address malicious cyber activities, while being less burdensome for providers.

An ADP, like the one described, will also help foster a more collaborative environment between government and industry and international partners and allies, which is essential for these anti-cyber abuse measures to be successful. It is rare for any private company or governmental entity to have all the relevant data at hand. Instead, each will have pieces of information that help build a more fulsome picture of possible suspicious activities. A close partnership between the public and private sectors, therefore, remains essential to address these threats.

******

SIIA thanks BIS for considering our views. We look forward to continuing our engagement with BIS on this important issue and would welcome the opportunity to answer any additional questions that the Bureau may have.

Please direct any questions to Paul Lekas (plekas@siia.net) or Morten C. Skroejer (mskroejer@siia.net).

Respectfully submitted,

Paul Lekas
Senior Vice President, Global Public Policy

Morten C. Skroejer
Senor Director, Technology Competition Policy

[26] *Supra* note 1 §7.306(b).