BSA Comments on Department of Commerce
Request for Comments on Proposed Rule
Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities
April 25, 2024

BSA appreciates the opportunity to provide comments on the Department of Commerce's (Department) Bureau of Industry and Security's (BIS) Notice of Proposed Rulemaking (NPRM or Proposed Rule) to implement aspects of the Executive Order on Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities signed by President Trump on January 19, 2021 (EO 13984) and the Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence signed by President Biden on October 20, 2023 (EO 14110).

BSA is the leading advocate for the global software industry.[1] BSA members are at the forefront of developing and deploying cutting-edge services — including AI — and their products are used by businesses and government agencies around the globe and across every sector of the economy. For example, BSA members provide tools including cloud storage and data processing services, customer relationship management software, human resource management programs, identity management services, cybersecurity services, and collaboration software. BSA members are on the leading edge of providing cloud-based and AI-enabled products and services. As a result, they have unique insights into the technology's tremendous potential to spur digital transformation and the policies that can best support the responsible and effective use of AI and cloud services.

Our comments focus on eight aspects of the Proposed Rule. We recommend the Department:

- Consider separating implementation of EO 13984 (on malicious cyber activities) and EO 14110 (on AI), given their different contexts and goals;
- Clarify the definition of Infrastructure-as-a-Service (IaaS) products, to clearly exclude Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) products;
- Improve procedural and substantive requirements for customer identification programs (CIPs);
- Encourage companies to adopt Abuse of IaaS Products Deterrence Programs by improving exceptions to the CIP requirements for companies with such programs;
- Add important factors the Secretary must consider before implementing a special measure;
- Revise the AI reporting obligations to create clear definitions and thresholds and avoid violating the Stored Communications Act;

[1] BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Okta, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.

- Engage international partners to ensure they understand the targeted nature of the rule and develop an international framework for advanced model reporting; and

- Avoid imposing criminal penalties.

I. The Department Should Separate the Implementation of EO 13984 and EO 14110

The Proposed Rule implements both EO 13984 and EO 14110.

Each of these efforts proposes requiring a company to obtain, report, and retain information about its customers. However, EO 13984 was signed by President Trump to address a national emergency created by malicious actors stealing intellectual property and sensitive data and targeting US critical infrastructure through malicious cyber-enabled activities; deter foreign malicious actors from using US IaaS offerings to launch malicious cyber activity; and assist in the investigation of such malicious activity. In short, EO 13984 is aimed at the misuse of US IaaS.

By contrast, EO 14110 aims to "advance and govern the development and use of AI in accordance with eight guiding principles and priorities" and is intended to ensure the availability of safe, secure, and trustworthy AI through, among other activities, managing the legitimate use of US IaaS products to train AI models. We believe that know-your-customer requirements can play an important role in achieving these objectives, if they are targeted at, and well calibrated to, advancing visibility of the most highly capable models.

Despite each of these EOs proposing to require a subset of companies to "know your customer," the EOs are significantly different. BSA recommends the Department implement EOs 13984 and 14110 in separate regulatory processes.

II. The Department Should Clarify the Definition of IaaS Product

Section 7.301 of the Proposed Rule defines IaaS product as "a product or service offered to a consumer . . . that provides processing, storage, networks, or other fundamental computing resources, and with which the consumer is able to deploy and use software that is not predefined, including operating systems and applications."

This definition appears to exclude PaaS and SaaS offerings, including serverless offerings, because PaaS and SaaS offerings are predefined, i.e., a user of a PaaS or SaaS offering uses the platform or software provided by the PaaS or SaaS provider. BSA supports this approach. Excluding PaaS and SaaS offerings aligns with the purpose of EO 13984, because the risks associated with malicious actors using predefined software in PaaS and SaaS products are low, and the benefits of reports from PaaS and SaaS providers would be of limited value. However, further clarification that PaaS and SaaS offerings, which often include provisioning of the underlying computing resources which may be controlled and managed by the PaaS or SaaS provider, are not covered by the regulations would provide additional certainty, thereby creating the conditions for economic growth. Importantly, it would help ensure that US PaaS and SaaS providers aren't placed at a competitive disadvantage with European and Asian companies not subject to the same or similar types of requirements.

BSA recommends the final rule more explicitly indicate that SaaS and PaaS offerings are excluded from the definition of IaaS product by adding the following language to the IaaS product definition:

Platform as a Service (PaaS) offerings (platform services provided primarily for the purpose of utilizing the PaaS provider's integrated software tools and applications, typically also including provisioning of underlying computing resources controlled and managed by the PaaS provider) and Software as a Service (SaaS) offerings (software services provided by allowing users to connect to and use cloud-based applications over the internet) are not included in the definition of Infrastructure-as-a-Service products.

We also note that the Proposed Rule not only applies to US IaaS providers' private sector customers but also their government customers. Considering the relative risk with respect to certain governments, and

carving out those that are lower risk from the requirements, is one way in which the Department could more narrowly tailor the Proposed Rule to both facilitate implementation and achieve the Department's objectives.

Furthermore, for the AI reporting requirements, consider applying them only when a foreign customer is accessing a very large, and defined, amount of training compute, for example the 10^26 FLOPs set out in the AI EO. Focusing reporting requirements on foreign customers accessing a large and defined amount of compute would advance the Department's goal of having visibility into where only the most highly capable models are being developed, by focusing on access to large scale training infrastructure needed to train them, while creating a more targeted and implementable rule. We recognize that use of a compute threshold is not a perfect solution. It could be overinclusive given the lack of technical ability for IaaS providers to distinguish among the purposes for using large compute capabilities, and underinclusive because it does not include powerful smaller models. However, it is a more effective approach for identifying models with the most significant capabilities and a more objective benchmark than the subjective considerations included in the Proposed Rule. Moreover, for the reasons outlined in Section VI, any reporting requirements should be placed directly on customers.

III. The Department Should Improve the Process and Substance of the Customer Identification Program (CIP).

The Proposed Rule imposes overly broad requirements on US IaaS providers, and the Department can instead achieve its goals while reducing burdens on US companies.

The CIP requires IaaS providers to include "how the provider will verify the identity of its foreign customers." In practice, this will require US IaaS providers to undertake steps to verify the identity of all their customers to determine which customers are foreign and which are domestic. This undertaking would require, among other efforts, a manual evaluation of documents in different languages and require IaaS providers to search for ownership information for all customers without regard to the size, industry, public company status, or other factors that may impact a customer's risk profile. This evaluation would be difficult and expensive for companies to scale because it likely goes far beyond existing company processes. These resource intensive requirements will not be required of international competitors, hampering US IaaS providers' ability to compete. If the Department maintains these overarching CIP obligations, it is important to more clearly focus the CIP's requirements to avoid unnecessarily broad application, as recommended below.

A. The Final Rule Should Target the CIP Reporting Requirements to Information That Will Address Malicious Cyber Activity.

Section 7.304(a)(2)(i) of the Proposed Rule requires each US IaaS provider to submit a CIP certification form to the Department with certain information. Under the Proposed Rule, that information is to include "a description of the IaaS provider's service offerings and customer bases in foreign jurisdiction" and, pursuant to (a)(2)(vi), "[t]he number of IaaS customers."

These provisions seek broad information about IaaS providers' business activities that will not help prevent foreign persons from using US IaaS products to conduct malicious cyber-enabled activity or otherwise safeguard the national security of the United States. Malicious, cyber-enabled activity is not undertaken by customer bases or groups of customers, but by specific malicious actors. The US Government collecting broad information on US IaaS providers will undermine trust both in US IaaS providers specifically and other US business generally. This approach will also undermine the US Government's advocacy against other governments seeking broad information from businesses operating in their jurisdictions or in the United States.

BSA recommends the final rule remove these reporting requirements.

B. The Final Rule Should Allow a US IaaS Provider to Grant Access to Accounts Prior to Successful Identity Verification.

The NPRM asks whether the Department should allow US IaaS providers to grant customers access to accounts prior to successful identity verification.

If customers cannot access an account provided by a US IaaS provider but instead are made to wait until the customer's identity can be verified, it creates a significant barrier to using a US IaaS provider that will not exist for other IaaS providers and therefore will make non-US IaaS providers comparatively more attractive. In so doing, the Department's efforts to address the national emergency declared in January 2021, may negatively impact US businesses and in turn harm US economic and national security as customers may shift to foreign providers.

BSA recommends the final rule allow US IaaS providers to grant customers access to accounts while they verify the customer's identity.

C. The Final Rule Should Not Require a US IaaS Provider to Obtain the Address or Location from Which a Customer Will Use the IaaS Product.

Section 7.302(d)(1)(iii)(B) of the Proposed Rule requires a US IaaS provider to obtain the address or location "from which the IaaS product will be used" as part of the CIP.

It is not reasonable or practical for a US IaaS provider to obtain the address or location from which a customer will use the IaaS product. One key feature of IaaS products is that they provide customers the ability to access services from multiple different locations. As a result, a single customer may access the IaaS product from dozens (or more) locations at the same time, rendering this requirement impractical.

BSA recommends the final rule remove the requirement to obtain the address from which the IaaS product will be used.

D. The Final Rule Should Require a US IaaS Provider to Retain Records for 90 Days.

Section 7.302(e)(2) of the Proposed Rule would require a US IaaS provider to retain records for two years after an account was last accessed or closed. The Department believes this is necessary to allow a law enforcement agency the ability to access this information should it suspect malicious actors used the account.

Collecting and retaining information longer than necessary is a bad security and privacy practice and makes the holder of that information a target for malicious activity. Minimizing the collection and retention of data can help reduce the risk of an IaaS provider being targeted and its customers' information from being stolen. For example, NIST Special Publication 800-53 notes that the principle of minimization suggests that organizations only collect information that is directly relevant and necessary to accomplish their purposes and only retain that information for as long as it is necessary. It further states: "Although policies to control for authorized use can be applied to information once it is collected, minimizing the collection of information that is not needed mitigates privacy risk." Here, the Proposed Rule would require the collection and retention of information beyond what the Department's own bureau's guidance suggests.

Requiring companies to retain customer information for two years may also create unnecessary tension with like-minded allies that prioritize the principle of data minimization. This can hinder the Department's own efforts to facilitate the flow of information across borders, for example between the United States and the EU. Further, the proposed requirements risk subordinating the Department's mission "to create the conditions for economic growth and opportunity for all communities" to the separate mission of law enforcement agencies, which can harm the ability of US IaaS providers to serve customers around the world.

BSA recommends the final rule reduce the time a US IaaS provider is required to retain records to a maximum of 90 days.

E. The Final Rule Should Not Require US IaaS Providers to Determine if a Foreign Reseller Has Made a Good-Faith Effort.

Section 7.303(e) requires US IaaS providers to ensure that any foreign reseller maintains a CIP that complies with requirements in Section 7.302(c) – (e) and "upon receipt of evidence that indicates the failure of a foreign reseller to maintain or implement a CIP or the lack of good-faith efforts by the foreign reseller to prevent the use of U.S. IaaS products for malicious cyber-enabled activities" close the foreign reseller account and report the activity to relevant authorities. The US IaaS provider must also terminate the relationship with the reseller in 30 days if it is aware that the foreign reseller has not remediated the issue, or if continuation of the relationship otherwise increases the risk its US IaaS products may be used for malicious cyber-enabled activity.

US IaaS providers do not have visibility into a reseller's environment and are therefore not in a position to determine or monitor if a reseller is making a good-faith effort to prevent the misuse of US IaaS products. In addition, it is not clear how an IaaS provider would assess the risk that a reseller relationship increases the risk that its IaaS products will be misused.

BSA recommends the final rule remove the requirement to close a reseller account based on indications that the reseller fails to make a good-faith effort to prevent the use of US IaaS products for malicious activity.

F. The Final Rule Should Require a US IaaS Provider to Certify Its CIP When It Has Experienced a Significant Change.

Section 7.304(b) of the Proposed Rule requires a US IaaS provider to certify its CIP annually, and Section 7.304(c) requires a US IaaS provider to notify the Department if it has experienced a significant change to its CIP.

These provisions will create significant new work, not just for IaaS providers, but also for the Department. To review annual CIP certifications, the Department would likely have to hire or contract numerous employees, even though the vast majority of annual certifications would not contain significant new information. The Department can more efficiently accomplish its goals and avoid unduly burdensome reporting requirements for US IaaS providers by avoiding an annual certification requirement. More importantly, these certifications will not prevent the activity the Department seeks to curb. Aligning on prudent and robust cybersecurity policies, controls, or certifications is more likely to address the Department's policy objective.

BSA recommends the final rule require a US IaaS provider only to update the Department when there has been a significant change to its CIP.

IV. The Department Should Both Incentivize Use of and Make the Process for Approving, Denying, or Revoking an ADP Request Exemption Clear and Robust.

Section 7.306 of the Proposed Rule authorizes the Secretary to exempt a US IaaS provider from the CIP requirements in Section 7.303 and 7.304, if the Secretary finds that the US IaaS provider has implemented "security best practices to otherwise deter abuse of IaaS products" through establishing an Abuse of IaaS Products Deterrence Program (ADP)." The Proposed Rule creates procedures for a US IaaS provider to request an exemption from the CIP requirements, creates requirements for the IaaS provider to maintain its exemption, and provides that the Department may revoke the exemption "at any time."

BSA applauds the proposal to include an exemption based on best practices. The President's National Security Telecommunications Advisory Committee (NSTAC) NSTAC Report to The President identified this approach as a path to mitigate abuse of US infrastructure.

IaaS providers using best practices will be more effective and efficient at improving security than companies collecting and retaining information about their customers. However, the Proposed Rule's requirement related to the ADP is vague in key respects. First, it is unclear what controls are necessary to obtain the exemption. We encourage the Department to leverage existing standards to establish the

appropriate benchmark. Second, the Proposed Rule creates significant uncertainty around the Department's expectations, for example, how long the Department may take to approve or deny a US IaaS provider's request, the obligations a US IaaS provider has between the time it makes the request and the time the Department makes a determination, how the Department will share with a US IaaS provider information about the basis for its determination, or how a US IaaS provider can appeal an inappropriate determination. This uncertainty creates barriers to companies investing in this program.

Further, BSA recommends the final rule include key standards that a US IaaS provider must meet (e.g. ISO cybersecurity certifications) to be eligible for exemption rather than requiring a formal application for exemption. This would reduce the administration burden for the Department while still creating a framework for the Department to verify the standards are met when it elects to do so.

In the absence of a "self-serve exemption," BSA recommends that the final rule: (1) provide a timeline to grant or deny a US IaaS provider's request for an exemption, (2) exempt a US IaaS provider from CIP requirements pending the Department's approval or denial of its request; (3) provide a US IaaS provider documentation of a denial or revocation of its ADP, and (4) create an opportunity for the US IaaS provider to appeal or remedy any issues the Department identifies.

V. The Department Should Add Important Factors the Secretary is Required to Consider Before Implementing a Special Measure.

Section 7.307(b)(4) of the Proposed Rule contains factors the Secretary must consider before imposing a special measure.

In rare circumstances, a special measure may be necessary to accomplish the goals of the Executive Orders. However, those circumstances should be limited. The Secretary should not impose a special measure prior to considering and exhausting other options to achieve the same goals and the impacts of a special measure on US IaaS providers and the US economy.

In addition to factors set out in the Proposed Rule, the Secretary should consider whether (1) the US Government has exhausted diplomatic efforts to address the risks identified and (2) the imposition of a special measure would lead to an increase in the use of foreign IaaS products, which would ultimately harm the US economy and make it more difficult to identify, address, or disrupt malicious activities.

BSA recommends that the final rule require the Secretary to consider these factors before imposing a special measure.

VI. The Department Should Revise the AI Provisions to Create Clear Thresholds and Avoid Violating the Stored Communications Act.

Section 7.308 of the Proposed Rule requires IaaS providers to report information about transactions involving foreign persons that could result in the training of a "large AI model with potential capabilities that could be used in malicious cyber-enabled activity." These obligations create several concerns, including: (1) they lack clear thresholds, (2) they appear to create obligations that would violate the Stored Communications Act, and (3) they require providers to submit information that a provider often does not have.

A. The Proposed Rule Does Not Provide Sufficiently Clear, Risk-Based Thresholds for Reporting Requirements Related to Large AI Models.

The Proposed Rule's definition of a large AI model includes models that have "technical parameters of concern," aid in malicious cyber activities, including social engineering attacks and misinformation, and meet the technical conditions identified in forthcoming rules issued by the Department.

The definition is flawed for several reasons:

- First, the reference to "technical parameters of concern" is imprecise and does not provide concrete information about the parameters that would pose risks of malicious activity. Further, even where the Proposed Rule references specific quantities of parameters, the Department has

still failed to demonstrate that the model's number of parameters is the appropriate measure of potential risk.

- Second, the Proposed Rule presumes that an IaaS provider would have insight into whether AI training activities could result in social engineering attacks or misinformation. As discussed further below, IaaS providers don't typically have access to information that would alert them of these activities.

- Third, the Proposed Rule allows the Department to establish technical conditions without applying any clear risk-based standards.

Further, the AI EO directs the Department to revise the conditions as necessary and appropriate, which means IaaS providers cannot rely on predictable benchmarks.

BSA recommends that the final rule revise the definition of a large AI model that triggers the reporting requirements and use a compute-based threshold, for example the 10^26 FLOP threshold outlined in the AI EO. Given the connection between compute used in training and model performance, compute-based thresholds have value in helping identify highly capable models. Using this threshold would help focus the rule on only models that likely have the most advanced capabilities. It would also advance consistency across this rule and the rest of the AI EO.

B. The Proposed Rule Appears to Violate the Stored Communications Act.

Section 7.308 of the Proposed Rule's reporting requirements for large AI model training also appear to conflict with the Stored Communications Act (SCA).

The SCA protects the privacy of electronic records and communications by prohibiting companies that provide either electronic communications services or remote computing services (collectively, "providers") from disclosing information they hold on or about their subscribers, unless one of the statute's narrow exceptions applies. The SCA therefore presumes such information cannot be shared — and specifically prohibits providers from disclosing "a record or other information pertaining to a subscriber or customer of such service . . . to any governmental entity."[2] However, the SCA creates narrow exceptions that allow providers to disclose specific types of information to government entities pursuant to specific forms of legal process. Under the SCA:

- Providers may disclose *basic subscriber information* to a government entity pursuant to specific types of subpoenas.[3]

- Providers may disclose *non-content information* to a government entity pursuant to a court order issued under 18 U.S.C. 2703(d).

- Providers may disclose *content information* to a government entity pursuant to a warrant.

In addition to allowing providers to share information with government entities pursuant to legal process, the SCA also creates narrow exceptions for disclosures in certain emergencies, disclosures made with consent, or disclosures necessarily incident to the provision of services, among other narrow exceptions.[4]

---

[2] 18 U.S.C. 2702(a)(3).
[3] The SCA specifies that these subpoenas must be either: (1) an administrative subpoena authorized by federal or state statute, (2) a federal or state grand jury subpoena, or (3) a trial subpoena. See 18 U.S.C. 2703(c)(2).
[4] The SCA's other exceptions do not appear to apply to any disclosures required by the Draft Regulations. Under 18 U.S.C. 2702(b), providers may disclose the *content* of communications only in specific and narrow circumstances, namely: (1) to an addresses or intended recipient, or an agent of such addressee or intended recipient; (2) as authorized by the SCA and specific federal wiretapping laws; (3) with the consent of the originator, addressee, intended recipient, or subscriber; (4) to a person employed or authorized or whose facilities are used to forward such communication to its destination; (5) as may be necessarily incident to the rendition of the service or to protect the rights or property of the provider; 6) to the National Cetner for Missing and Exploited Children, in

None of these exceptions appear to contemplate providing information to a government agency in the manner contemplated by the Proposed Rule.

The Proposed Rule simply does not account for the SCA's prohibition on disclosing information. Under Section 7.308 of the Proposed Rule, US IaaS providers must submit a report to the Department when they have "knowledge" of certain transactions — which include information that is clearly protected by the SCA) — without the legal process required by the SCA. Specifically:

- Submitting an initial report with information about a foreign person requires disclosing basic subscriber information protected by the SCA. Under the Proposed Rule, US IaaS providers are to file initial reports that contain specific information about a relevant foreign person, including the name of the foreign customer, the address of that customer, its principal place of business, the means and source of payment, email address, telephonic contact information, and IP addresses used for access or administration and the date and time of each such access or administrative action. These categories of information appear to closely align with the categories of basic subscriber information protected by the SCA: name; address; local and long distance telephone connection records, or records of session times and durations; length of service (including start date) and types of services utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and means and source of payment for such service. *The SCA prohibits providers from disclosing these categories of information to a government entity absent an administrative subpoena, grand jury subpoena, or trial subpoena*.

- Submitting an initial report with information about the training requires disclosing either (or both) non-content information and content information protected by the SCA. Under the Proposed Rule, IaaS providers' initial reports are also to contain specific information about certain training runs, including the estimated number of computational operations used in the training run, the anticipated start date and completion date of the training run, information on the training practices, and information on the customers' cybersecurity practices. To the extent this information reflects the "substance, purport, or meaning" of a wire, oral, or electronic communication, the SCA's protections for content information would apply, and a provider would be barred from disclosing this information to a government entity absent a warrant (or other statutory exception).[5] If the information is not content, then the SCA's protections for non-content would apply and the provider would be barred from disclosing the information to a government entity absent a court order issued under 18 U.S.C. 2703(d) (or other statutory exception). *In either case, the SCA would prohibit providers from disclosing this information absent legal process or another exception under the SCA.*

The Proposed Rule contemplates that providers not only share information about a specific subscriber in these initial reports, but also that providers continue to submit further information to the Department. For example, the Proposed Rule requires providers to submit follow-up reports with "all information responsive" to a request from the Department and contemplates that BIS may request a provider submit "additional information pertaining to activities or risks that present concerns to US national security." Once again, these provisions of the Proposed Rule do not address the SCA's protections for that information — and appear to require providers to disclose information for which the SCA requires legal process.

---

connection with a report submitted under federal laws on child sexual exploitation; (7) to a law enforcement agency only if the contents were inadvertently obtained by the provider and appear to pertain to the commission of a crime, (8) to a governmental entity if the provider in good faith believes that an emergency involving danger of death or serious physical injury to a person requires disclosure without delay, and (9) to a foreign government pursuant to a request issued under the CLOUD Act. 18 U.S.C. 2702(b). For non-content information, the SCA creates a somewhat broader set of exceptions, which allow providers to disclose *non-content* to "any person other than a governmental entity." 18 U.S.C. 2702(c)(6).

[5] See 18 U.S.C. 2510(8) (defining the content of communications).

Although we appreciate the Proposed Rule's important goal of addressing legitimate national security concerns, it is critical that the Proposed Rule be revised to account for the SCA's clear requirements for providers to protect electronic information.

BSA strongly recommends the Department revise the Proposed Rule's approach to these reporting requirements, to avoid creating a conflict with the SCA. One option that may help navigate challenges of privacy and confidentiality is to both limit the covered information to the amount of compute and focus the rule on foreign customers self-reporting to the US Government when they are accessing this amount of compute. Under this approach, IaaS Providers could simply check that the foreign customer has provided the required notification, rather than collecting the required information from the customer on model development or reporting information protected by the SCA to the US Government.

C. The Proposed Rule Requires IaaS Providers to Submit Information They Do Not Have.

Even if the Proposed Rule provided a clearer reporting threshold and did not violate the SCA, Section 7.308(d)(1)(ii) of the Proposed Rule asks IaaS providers to give the Department information they do not have.

Many IaaS providers ensure they have limited access to their customers data, in order to protect the privacy and security of that data. As a result, US IaaS providers often do not have detailed insight into the data stored on their platform, or their business customers' practices in handling that data. Indeed, many IaaS providers are subject to contractual limitations that prevent them from accessing their customers' data, except in narrow circumstances.

The Proposed Rule does not account for the limited information available to many IaaS providers. For example, the Proposed Rule requires a US IaaS provider to report information about its customer's cybersecurity practices, including incidents involving unauthorized access to model weights or source code. However, IaaS providers generally do not have access to this information because they do not have visibility into the customer environment. In fact, IaaS providers' contractual arrangements and some local laws contain strict rules that limit their insight into their customers' data. Moreover, IaaS providers lack the technical means for providing some of the information the Proposed Rule requires. Further, Section 7.308(e) of the Proposed Rule authorizes the Department to request additional information about activities or risks that present concerns to national security. This additional authority is vague and overbroad, and will likely also implicate other information that goes beyond the scope of information that IaaS providers collect in connection with their provision of the service.

BSA recommends the final rule remove these requirements.

D. The US Government Should Work With Partners to Share Key Objectives of the Rule and Develop an International Framework for Advanced Model Reporting.

Engaging partner countries in the EU and elsewhere would help them understand the Department's intent to focus the rule tightly on only the most capable models. As the rule is finalized, the US Government should also work with these foreign partners to develop an international framework for model reporting, with model developers reporting compute information directly to their home governments and partner governments sharing information between each other to ensure consistent approaches globally.

VII. The Department Should Not Impose Criminal Penalties.

Section 7.309 of the Proposed Rule would create criminal penalties, including fines of up to $1,000,000 and imprisonment for up to 20 years.

While effective penalties are important elements of any law, imposing criminal penalties in this context is disproportionate and unwarranted. To be effective, penalties should be proportionate to the activities they seek to deter or encourage. One unintended consequence of the proposed disproportionate criminal penalties is that they will undermine or reduce the legitimate business activities of US IaaS providers. US IaaS providers' commercial success contributes meaningfully to US economic and national security, as well as the economic and national security of US allies. Consequently, by imposing criminal penalties, the

Department may introduce new economic challenges by making the use of foreign IaaS providers comparatively more attractive.

Here, the Proposed Rule also contains civil penalties of "$250,000 per violation . . . or an amount that is twice the amount of the transaction that is the basis for the violation" subject to the adjustment pursuant to the Federal Civil Penalties Inflation Adjustment Act of 1990. These civil penalties are more than sufficient to ensure US IaaS providers meet their legal obligations.

BSA strongly recommends the final rule not impose criminal penalties.

* * *

Thank you for the opportunity to provide comments on the Proposed Rule. BSA looks forward to serving as a resource as you continue to consider these important issues.