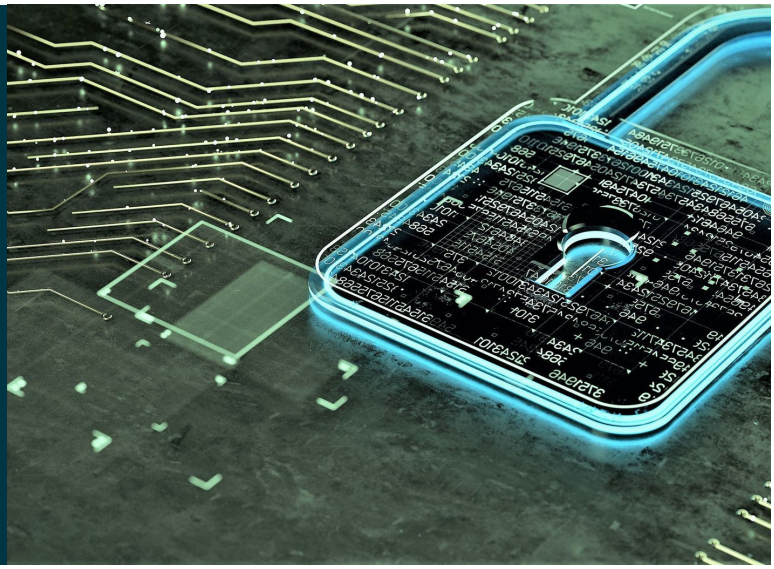
WILSON SONSINI

First Proposed Rules Under Biden AI Order Issued as Part of Larger New Customer Cyberthreat Disclosure Requirements for Cloud Computing Providers



CONTRIBUTORS

Joshua F. Gruenspecht

Kara D. Millard

Madeline Cimino

ALERTS

February 1, 2024

On January 29, 2024, the U.S. Department of Commerce (Commerce) issued a notice of proposed rulemaking (NPRM) seeking comment on draft rules establishing customer information collection and reporting obligations for certain U.S. cloud services providers. The NPRM proposes reporting requirements for customer development of large AI models that constitute the first proposed rules implementing President Biden's sweeping artificial intelligence (AI) Executive Order (EO) (covered in further detail here). More generally, the NPRM proposes to add to the existing ICTS ruleset established under an earlier Trump EO (which we discuss here) by requiring U.S. cloud computing services to verify customer identities and report various kinds of accounts and activity to Commerce. Commerce may then use these new authorities to block or condition certain customers' use of cloud computing services if it believes those services may be used in malicious cyber-enabled activity.

The proposed rules, once finalized, will have their most immediate impact on U.S. Infrastructure as a Service (IaaS) providers—i.e., the defined set of cloud computing services providers with customer information collection and reporting obligations. The NPRM appears to suggest that the set of covered IaaS providers will be comparatively narrow—e.g., well-known hyperscale cloud providers, certain data center operators, and certain providers of services related to core internet functioning. These IaaS providers will also be the ones responsible for determining whether customers may be training "a large AI model with potential capabilities that could be used in malicious cyber-enabled activity." Resellers of IaaS services will also face related customer information collection and reporting requirements. Both IaaS providers and resellers, therefore, may have an interest in submitting comments to Commerce on the NPRM to influence the shape of the final rules.

The much broader set of customers and cloud software companies that rely on IaaS services will be less immediately affected. However, users of cloud computing services will face more extensive reporting requirements (not unlike Know-Your-Customer (KYC) reporting required under U.S. banking or anti-money laundering regulations) when setting up accounts with their service providers. Foreign customers of U.S. IaaS providers, in particular, will be likely to have to answer more significant questions about their ownership and usage of IaaS services.

Understanding the New Rules: What IaaS Providers Must Collect and Report, and How Commerce Can Respond

The draft regulations require U.S. IaaS providers to maintain and implement written Customer Identification Programs (CIPs) appropriate for the IaaS providers' size, type of products offered, and relevant risks. Resellers of U.S. IaaS products may use or adopt the initial U.S. IaaS provider's CIP to achieve compliance. The CIP must include risk-based procedures for verifying the identity of each foreign customer to a reasonable belief standard. The CIP procedures must also provide U.S. IaaS providers or foreign resellers of U.S. IaaS products with a sound basis to verify the true identity of their customer and beneficial owners and will be required to reflect reasonable due diligence efforts.

Certain IaaS providers may also be exempted from the CIP requirements by Commerce under specified circumstances.

As proposed, U.S. IaaS providers that contract with, enable, or otherwise allow foreign resellers to resell their U.S. IaaS products must also ensure that their foreign resellers maintain and implement written CIPs. If foreign resellers fail to do so, the U.S. IaaS provider must close the foreign reseller account and, if relevant, to report the suspected or actual malicious cyber-enabled activity to relevant authorities.

In addition, each U.S. IaaS provider must notify Commerce of implementation of its CIP and the CIPs of any foreign reseller of its U.S. IaaS products. U.S. IaaS providers will be required to certify their CIPs on an annual basis. Under the NPRM, these reports will include detailed information on the IaaS providers' services, users, and procedures for reporting suspected or actual malicious cyber-activity. Commerce will have the right to perform compliance assessments on IaaS providers as it deems necessary.

The NPRM also proposes that IaaS providers directly report certain customer activity to Commerce when those customers use IaaS services to train large AI. In particular, U.S. IaaS providers must report to Commerce in the event they gain knowledge of transactions by, for, or on behalf of a foreign person which could result in the training of a large AI model with potential to be used in malicious cyber-enabled activity.

More generally, the draft regulations also enable Commerce to use special measures if reasonable grounds conclude that a foreign jurisdiction or foreign person is conducting malicious cyber-enabled activities using a particular U.S. IaaS provider's products. Commerce may prohibit or impose conditions on the opening and maintaining of accounts, including reseller accounts, by:

- any foreign person located in a foreign jurisdiction with a significant number of persons offering U.S. IaaS products that are obtained or used for perpetrating malicious cyber-enabled activities; or
- a foreign person found to be obtaining or offering U.S. IaaS products for use in malicious cyber-enabled activities.

Finally, the NPRM states that failure to comply with the rules can subject the noncompliant actor to civil penalties, criminal fines, and/or up to 20 years in prison.

Implications for IaaS Providers, Resellers, and Customers

While IaaS customers will face new diligence questions from their service providers' CIP programs, the bulk of the new proposed rules will fall on IaaS providers and their resellers. As a result, the most critical definition in the NPRM is the proposed definition of IaaS products, which is adopted directly from the Trump administration EO on ICTS. That draft definition appears to cover a relatively narrow range of service offerings—e.g., in part, those "with which the customer is able to deploy and run software that is not predefined, including operating systems and applications." That clause of the definition suggests that software-as-a-service (SaaS) companies that offer business services or spreadsheet processing in the cloud would not be covered, given that those are predefined tasks. Indeed, the NPRM itself recognizes the tension between a broad definition of IaaS and potentially impinging on the wider world of SaaS platforms.

However, elsewhere in the NPRM, Commerce suggests that providers of various internet infrastructure services—e.g., proxy services and domain name resolution services—would be considered IaaS providers under the proposed definition. As such services are used by customers to perform predefined tasks—and not, e.g., run an operating system or other arbitrary code—Commerce may end up believing a wider array of cloud service providers must adhere to its rules. Casting such a wide net, while seemingly part of a well-intentioned effort to mitigate foreign cyber risk, will likely pull smaller companies into this complex set of regulatory obligations.

Commerce's proposed definition of "large AI model with potential capabilities that could be used in malicious cyber-enabled activity" faces similar issues due to its general language, which potentially covers *any* sufficiently large AI model. That definition first includes the Biden AI EO definition of a dual-use foundation model, which is already broad, and then adds a series of other criteria that may cause an AI model to be covered, including criteria to be set forth in future published regulations. Ultimately, if this set of models is broadly defined, Commerce may end up receiving reports from IaaS providers with respect to nearly every foreign party training an AI model.

Companies providing large-scale cloud services, internet infrastructure services, large-scale AI-focused compute services, or other services at risk for being considered IaaS may wish to consider submitting comments on the NPRM. Commerce has requested that all comments be submitted by April 29, 2024.

We will continue to monitor developments both in the ICTS rules applicable to IaaS providers and in other regulations to be developed under the Biden AI EO. If you have any questions regarding the proposed rules, please contact Joshua Gruenspecht, Stephen Heifetz, Seth Cowell, Demian Ahn, Kara Millard, Madeline Cimino, or any other member of the firm's national security practice, privacy and cybersecurity practice, or artificial intelligence and machine learning working group.