UNITED STATES DEPARTMENT OF COMMERCE
Bureau of Industry and Security
1401 Constitution Avenue, Suite 3896
Washington, DC 20230

January 22, 2024

MEMORANDUM FOR: Dominic Mancini
Deputy Director
Office of Information and Regulatory Affairs
Office of Management and Budget

FROM: Karen H. Nies-Vogel KNV
Director, Office of Exporter Services
Bureau of Industry and Security

SUBJECT: Request for OMB Emergency Review and Approval of Information Collection for the establishment of annual certification reporting requirements to take additional steps to address the national emergency with respect to significant malicious cyber-enabled activities

On behalf of the Bureau of Industry and Security (BIS), I am seeking approval for emergency Paperwork Reduction Act (PRA) clearances to allow the Department of Commerce (Department), as represented by BIS, to publish a Federal Register Notice on the notice of proposed rulemaking on *Taking Additional Steps To Address the National Emergency With Respect To Significant Malicious Cyber-Enabled Activities* (IaaS NPRM), which will include the addition of new annual certification reporting requirements for U.S. Infrastructure as a Service (IaaS) providers to certify their Customer Identification Programs (CIP) and the CIPs of their foreign resellers with the Department, as well as to report to the Department whenever a foreign person transacts with them to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity.

BACKGROUND

The IaaS NPRM, which BIS anticipates will be published on or after January 26, will require that U.S. IaaS providers meet annual reporting requirements, especially related to their provision of U.S. IaaS products to foreign customers or customers. The proposed rule would require each U.S. IaaS provider of IaaS products to submit certifications regarding its CIP and, if applicable, its foreign resellers' CIPs to BIS on an annual basis. BIS anticipates conducting compliance assessments of certain providers, as described in the proposed rule. BIS also anticipates receiving CIP certifications from most U.S. IaaS providers once per year.

The proposed rule would also require a U.S. IaaS provider of IaaS products to submit reports to BIS on an ad hoc basis whenever a foreign person transacts with that provider to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity. OICTS anticipates its definition of large AI training run will capture only the frontier edge of AI models, and thus expects the compliance burden of this provision to be relatively low. However, OICTS expects that the number of AI training-related reports will vary over time as the number of reportable transactions may grow as the number of actors developing advanced AI models grows.

BIS plans to encourage U.S. IaaS providers to submit documentation required by the proposed rule in electronic format via a web-based portal, the development of which is under discussion within BIS.

JUSTIFICATION

The collection of information is needed to meet requirements described in Executive Orders (EOs) 13894[1] and EO 14110.[2] EOs 13984 and 14110 seek to address, among other things, the vulnerability of U.S. IaaS products to exploitation by foreign malicious cyber actors, and misuse of U.S. IaaS by malicious foreign entities to enhance AI capabilities. The establishment of annual certification reporting requirements is an important part of implementing EOs 13984 and 14110 and will also allow for appropriate monitoring of the risk of abuse of U.S. IaaS products by malicious cyber actors.

The reporting requirements proposed in the IaaS NPRM take into consideration feedback received in public comment on the concepts in this rule in an advance notice of proposed rulemaking (86 FR 53018) (Sept. 24, 2021). The proposed rule also considers the U.S. National Cyber Security Strategy, (the Strategy) which recognizes the value of Know-Your-Customer (KYC) programs. The proposed Customer Identification Program (CIP) requirements within the IaaS NPRM seek to develop KYC industry standards for both U.S. IaaS providers and their foreign resellers. The Strategy states that all service providers must make reasonable attempts to secure the use of their infrastructure against abuse or other criminal behavior and that addressing known methods and indicators of malicious activity including through implementation of EO 13984 is a priority.

EO 13984 directs the Secretary of Commerce (Secretary) to propose regulations requiring U.S. IaaS providers of IaaS products to verify the identity of their foreign customers, along with procedures for the Secretary to grant exemptions, and authorizes special measures to deter foreign malicious cyber actors' use of U.S. IaaS products. EO 14110 further directs the Secretary to propose regulations that require providers of certain IaaS products to submit a report to the Secretary when a foreign person transacts with that provider or reseller to train a large Artificial Intelligence (AI) model with potential capabilities that could be used in malicious cyber-enabled activity. The Department is issuing an NPRM to solicit comment on proposed regulations to implement Sections 1, 2, and 5 of EO 13984 and Sections 4.2(c) and (d) of EO 14110.

[1] "Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities," (Jan. 19, 2021).

[2] "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" (Oct. 30, 2023).