SUPPORTING STATEMENT
U.S. Department of Commerce
Bureau of Industry and Security
Taking Additional Steps To Address the National Emergency With Respect To Significant Malicious Cyber-Enabled Activities
0694-xxxx

A. Justification

1. Explain the circumstances that make the collection of information necessary.

This emergency request for a new Information Collection is necessary due to Executive Order (EO) 13984, "Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities," (Jan. 19, 2021). This EO directs the Secretary of Commerce (Secretary) to propose regulations requiring U.S. Infrastructure as a Service (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, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" (Oct. 30, 2023) 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 of Commerce (Department) is issuing a notice of proposed rulemaking (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.

EOs 13984 and 14110 declare emergencies due to 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. These foreign malicious actors use U.S. IaaS products to quickly stand up, execute, and close out operations. This situation presents challenges for U.S. efforts to combat such activities, which efforts include obtaining information through the legal or judicial process before foreign malicious cyber actors' transition to other IaaS products and evidence of the malicious activity is lost.

The U.S. National Cyber Security Strategy (the Strategy) recognizes the value of Know-Your-Customer (KYC) rules, and 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.

Additionally, the large-scale AI model reporting requirements pursuant to EO 14410 respond to the emergence of high-performance computing infrastructure to which U.S. IaaS providers and foreign resellers provide virtual access as a service, and which foreign malicious actors could use

to train large AI models that can enable or automate malicious cyber activity. This has raised considerable concern about the lack of visibility into the identities of entities that transact with providers to engage in certain AI training runs.

2. Explain how, by whom, how frequently, and for what purpose the information will be used. If the information collected will be disseminated to the public or used to support information that will be disseminated to the public, then explain how the collection complies with all applicable Information Quality Guidelines.

The collected information will be used by BIS's Office of Information and Communications Technology and Services (OICTS) to monitor and enforce the CIP requirements described in EO 13984 and fulfill the information collection requirements regarding training runs for large AI models and foreign resellers described in EO 14110. 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 on certain providers, as described in the proposed rule. BIS anticipates receiving CIP certifications from most U.S. IaaS providers—estimated to number between 25 and 1,837 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 does not anticipate disseminating the collected information to the public.

3. Describe whether, and to what extent, the collection of information involves the use of automated, electronic, mechanical, or other technological techniques or other forms of information technology.

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.

4. Describe efforts to identify duplication.

Through consultations with other departments and agencies—including the Department of Defense, Department of Homeland Security, Department of Justice, Department of the Treasury, and Office of the Director of National Intelligence—BIS will avoid duplication of information being gathered. The information that BIS intends to collect under the proposed rule may not be available without the proposed rule's requirement for U.S. IaaS providers to establish and

maintain CIPs and submit related certifications. The proposed rule, and the Department's implementation thereof, is intended in part to ensure that U.S. IaaS providers will be positioned to furnish information about certain foreign customers if information is requested by other Departments or agencies.

5. If the collection of information involves small businesses or other small entities, describe the methods used to minimize burden.

Although certain U.S. IaaS providers are large businesses, most are "small businesses" as defined by the Small Business Administration and have fewer than 500 employees. In the case of small businesses that are resellers of U.S. IaaS products, the Department proposes in the rule to allow U.S. resellers, by agreement with a U.S. IaaS provider, to reference, use, rely on, or adopt the CIPs created by the U.S. IaaS provider to help minimize any compliance burdens on the reseller. The proposed rule would also allow any U.S. IaaS provider, including a small business, to apply for an exemption to the CIP requirements. The Department may grant an exemption where the provider establishes an Abuse of IaaS Products Deterrence Program, as described in the proposed rule. BIS may additionally conduct outreach events to U.S. IaaS providers, including small businesses, to provide guidance and answer questions regarding the submission of certification required by the proposed rule.

Additionally, BIS currently plans to use an annual certification and attestation process to limit the amount of high-burden, bulk information collected from U.S. businesses, such as annual submission of a complete and updated CIP. The annual certification requires only the submission of certain information about a company's CIP, as opposed to submission of the CIP or customer information. If a small business submits its annual certification form annually, thus remaining compliant, BIS would likely only need to request additional information from a small business or entity in certain cases of a compliance assessment where BIS would work directly with such an entity.

6. Describe the consequences to the Federal program or policy activities if the collection is not conducted or is conducted less frequently.

Without annual CIP certifications, BIS will lack visibility into U.S. IaaS providers' compliance with the requirements of the proposed rule. Such limited visibility could allow or result in U.S. IaaS providers not having information about foreign customers that may be needed to support law enforcement investigations and prosecutions of certain foreign persons' malicious cyber-enabled activities. Lack of visibility and a lax compliance environment could also result in the Department needing to issue broader and more frequent special measures to prevent cyber-enabled malicious activity in U.S. IaaS products. Lax compliance could also harm U.S. national security by limiting the degree to which CIPs raise the costs for certain foreign persons, specifically those seeking to engage in malicious cyber-enabled activities, to access and use U.S. IaaS products.

Without ad hoc reports regarding transactions to train large AI models, the Department and its partners across the U.S. government will lack visibility into potentially malicious uses of AI

conducted by foreign persons.

7. Explain any special circumstances that require the collection to be conducted in a manner inconsistent with OMB guidelines.

There are no special circumstances that will result in the collection of information in a manner inconsistent with the guidelines of 5 CFR 1320.6.

8. Provide information of the PRA Federal Register Notice that solicited public comments on the information collection prior to this submission. Summarize the public comments received in response to that notice and describe the actions taken by the agency in response to those comments. Describe the efforts to consult with persons outside the agency to obtain their views on the availability of data, frequency of collection, the clarity of instructions and recordkeeping, disclosure, or reporting format (if any), and on the data elements to be recorded, disclosed, or reported.

Prior to issuing this proposed rule, the Department sought and received public comment on the concepts in this rule in an advance notice of proposed rulemaking (ANPRM) (86 FR 53018) (Sept. 24, 2021). The Department received 21 comments to the ANPRM, and addresses those comments in this proposed rule. The Department plans to issue the current NPRM in question on January 26, 2024, and provide 90-day notice requesting public comment.

9. Explain any decisions to provide payments or gifts to respondents, other than remuneration of contractors or grantees.

This proposed rule will not involve any payment or gifts to persons require to submit documentation.

10. Describe any assurance of confidentiality provided to respondents and the basis for assurance in statute, regulation, or agency policy.

Although we did not develop any specific confidentiality provisions in this proposed rule, the Department is committed to protecting business proprietary and confidential information submitted. Some information collected under this rule would generally be considered to be confidential business information, as defined in 19 CFR 201.6, or proprietary information. When submitting such information, entities should notify the Department and provide the statutory basis for the claim of confidentiality. Note too that some information or documentary materials collected under this rule, not otherwise publicly or commercially available, will not be released publicly except to the extent required by law. Based on existing statutes, including the criminal provisions of 18 U.S.C. § 1905, federal employees disclosing confidential or business proprietary information may face civil and criminal penalties for doing so.

11. Provide additional justification for any questions of a sensitive nature, such as sexual behavior and attitudes, religious beliefs, and other matters that are commonly considered private.

Not applicable.

12. Provide an estimate in hours of the burden of the collection of information.

Public reporting burden for the reporting and recordkeeping requirements are estimated to average 245,778 hours for the initial learning, developing, and implementing a CIP for the relevant industry participants (897 respondents * 274 hours, Tables 1, 2, and 3). Thereafter, the Department estimates a public reporting burden of 84,494 hours to update and annually certify with the Department a CIP once it has been developed, as well as prepare the annual certification (929 respondents * 91 hours, Tables 4 and 5). The Department estimates a public reporting burden of 127,328 hours for the relevant industry participants to educate their foreign resellers on the rule and process reporting from and on foreign resellers and foreign customers (692 respondents * 184 hours, Tables 6 and 7). These estimates include the time for reviewing instructions, searching existing data sources, gathering the data needed, and completing and reviewing the collection of information.

13. Provide an estimate of the total annual cost burden to the respondents or record-keepers resulting from the collection (excluding the value of the burden hours in Question 12 above).

BIS anticipates that many, if not most, U.S. IaaS providers already have processes and equipment in place to maintain certain customer information, including some of the information required to be retained by the NPRM. Since no special equipment is required for this activity, BIS does not anticipate entities will incur much additional capitalized costs due to this proposed collection of information. Administrative processes may be necessary to ensure that records are maintained for two years, and then archived or otherwise destroyed based on individual entity policy and procedures, but these costs are already captured holistically in the burden of implementing a CIP in the response to question 12.

14. Provide estimates of annualized cost to the Federal government.

The total estimated cost specifically and only related to the receipt and collation of annual certification reports by U.S. IaaS providers to the U.S. government is $409,200 (500 notifications * 2 staff @ GS-12 salary ($102.30/hr) * average of 10 hours each to review for each notification). The $102.30 per hour cost estimate for this information collection is consistent with the GS-scale salary data for a GS-12 step 5.

15. Explain the reasons for any program changes or adjustments.

The number of anticipated responses and burden hours have not been adjusted, as the rule is not yet final and is therefore not in effect.

16. For collections whose results will be published, outline the plans for tabulation and publication.

BIS does not intend to publish the collected information.

17. If seeking approval to not display the expiration date for OMB approval of the information collection, explain the reasons why display would be inappropriate.

Not applicable.

18. Explain each exception to the certification statement.

Not applicable.

B. COLLECTIONS OF INFORMATION EMPLOYING STATISTICAL METHODS

Not applicable.