DEPARTMENT OF COMMERCE

15 CFR Part 7

[Docket No. 240119–0020]

RIN 0694–AJ35

Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities

AGENCY: Bureau of Industry and Security, Department of Commerce.

ACTION: Proposed rule; request for comments.

SUMMARY: The Executive order of January 19, 2021, ''Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities,'' 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 authorize special measures to deter foreign malicious cyber actors' use of U.S. IaaS products. The Executive order of October 30, 2023, ''Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,'' 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) issues this notice of proposed rulemaking (NPRM) to solicit comment on proposed regulations to implement those Executive orders.

DATES: Comments must be received April 29, 2024.

ADDRESSES: All comments must be submitted by one of the following methods:

- *By the Federal eRulemaking Portal: https://www.regulations.gov* at docket number DOC–2021–0007.
- *By email directly to: IaaScomments@bis.doc.gov.* Include ''E.O. 13984/E.O. 14110: NPRM'' in the subject line.
- *Instructions:* Comments sent by any other method or to any other address or individual, or received after the end of the comment period, may not be considered. For those seeking to submit confidential business information (CBI), please clearly mark such submissions as CBI and submit by email or via the Federal eRulemaking Portal, as instructed above. Each CBI submission must also contain a summary of the CBI, clearly marked as public, in sufficient detail to permit a reasonable understanding of the substance of the information for public consumption. Such summary information will be posted on *regulations.gov.*

FOR FURTHER INFORMATION CONTACT: Kellen Moriarty, U.S. Department of Commerce, telephone: (202) 482–1329, email: *IaaScomments@bis.doc.gov.* For media inquiries: Jeremy Horan, Office of Congressional and Public Affairs, Bureau of Industry and Security, U.S. Department of Commerce: *OCPA@bis.doc.gov.*

SUPPLEMENTARY INFORMATION:

I. Background

IaaS products offer customers the ability to run software and store data on servers offered for rent or lease without having to assume the direct maintenance and operating costs of those servers. Foreign malicious cyber actors have utilized U.S. IaaS products to commit intellectual property and sensitive data theft, to engage in covert espionage activities, and to threaten national security by targeting U.S. critical infrastructure. After carrying out such illicit activity, these actors can quickly move to replacement infrastructure offered by U.S. IaaS providers of U.S. IaaS products (''U.S. IaaS providers''). The temporary registration and ease of replacement for such services makes it more difficult for the government to track malicious actors. Additionally, the ability of malicious actors to use foreign-person resellers of U.S. IaaS products (''foreign resellers''), who might not track identity, hinders law enforcement's ability to obtain identifying information about malicious actors through service of compulsory legal process. This shift in adversary tradecraft also challenges the U.S. Government's ability to identify victims of malicious cyber activity and enable specific network defense and remediation efforts. Furthermore, the emergence of large-scale computing infrastructure—to which U.S. IaaS providers and foreign resellers provide access as a service, and which foreign malicious actors could use to train large AI models that can assist or automate their malicious cyber activity—has raised considerable concern about the identities of entities that transact with providers to engage in certain AI training runs.

To address these threats, the President issued E.O. 13984, ''Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities,'' which provides the Department with authority to require U.S. IaaS providers to verify the identity of foreign users of U.S. IaaS products, to issue standards and procedures that the Department may use to make a finding to exempt IaaS providers from such a requirement, to impose recordkeeping obligations with respect to foreign users of U.S. IaaS products, and to limit certain foreign actors' access to U.S. IaaS products in appropriate circumstances. The President subsequently issued E.O. 14110, ''Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,'' which calls for the Department to require U.S. IaaS providers to ensure that their foreign resellers verify the identity of foreign users. E.O. 14110 also provides the Department with authority to require U.S. IaaS providers submit a 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.

II. Introduction

E.O. 13984 and E.O. 14110 draw upon the President's authority from the Constitution and laws of the United States, including the International Emergency Economic Powers Act (IEEPA) (50 U.S.C. 1701 *et seq.*), the National Emergencies Act (NEA) (50 U.S.C. 1601, *et seq.*), and 3 U.S.C. 301. Section 1 of E.O. 13984 requires the Secretary to propose, for notice and comment, regulations that mandate that U.S. IaaS providers verify the identity of foreign persons that sign up for or maintain accounts that access or utilize U.S. IaaS providers' IaaS products or services (Accounts or Account)—that is, a know-your-customer program or Customer Identification Program (CIP). Under E.O. 13984, such a program must set forth the minimum standards for IaaS providers to verify the identity of a foreign person connected with the opening of an Account or the maintenance of an existing Account. The proposed regulations must include the types of documentation and procedures required to verify the identity of any foreign persons acting as a lessee or sub-lessee of these products or services; the records that IaaS providers must securely maintain regarding a foreign person that obtains an Account; and methods of limiting all third-party access to this collected information, except insofar as such access is otherwise consistent with E.O. 13984 and allowed under applicable law. Moreover, the proposed regulations

must consider the type of Account, methods of opening an Account, and the types of identifying information already available to IaaS providers that help accomplish the objectives of identifying foreign malicious cyber actors using any such products while also avoiding an undue burden on U.S. IaaS providers. They must also allow the Secretary, after consultation with the heads of various Federal agencies, to exempt any IaaS providers or any specific type of Account or lessee from the requirements of any regulation issued pursuant to this section, including due to a finding that the IaaS provider, Account, or lessee complies with security best practices to otherwise deter abuse of IaaS products.

Section 2 of E.O. 13984 requires the proposed regulations to allow the Secretary to use, as necessary, one of two special measures included in E.O. 13984 to require U.S. IaaS providers to prohibit or limit access to Accounts that foreign malicious cyber actors use to conduct malicious cyber-enabled activity. E.O. 13984 authorizes these measures if the Secretary, in consultation with heads of appropriate Federal agencies, finds that reasonable grounds exist to conclude that either: (i) a foreign jurisdiction has a significant number of foreign persons offering U.S. IaaS products that are, in turn, used for malicious cyber-enabled activities, or a significant number of foreign persons directly obtaining U.S. IaaS products and using them in malicious cyber-enabled activities; or (ii) a foreign person has established a pattern of conduct of offering U.S. IaaS products that are used for malicious cyber-enabled activities or directly obtaining U.S. IaaS products for use in malicious cyber-enabled activities. As further explained below, the Department would conduct an investigation before making any such finding under section 2 of E.O. 13894.

One special measure the Secretary could take would be to prohibit or impose conditions on opening or maintaining an Account with any IaaS provider by: (a) a foreign person located in a foreign jurisdiction that has a significant number of foreign persons offering U.S. IaaS products that are used for malicious cyber-enabled activities; or (b) on behalf of such a foreign person. The second special measure would allow the Secretary to prohibit or impose conditions on opening or maintaining an Account in the United States by any IaaS provider for, or on behalf of, a foreign person found to be offering U.S. IaaS products that are used for malicious cyber-enabled activities or on accounts opened directly by foreign persons who are known to obtain U.S. IaaS products for malicious cyber-enabled activities.

Section 4.2(c) of E.O. 14110 requires the Secretary to propose regulations requiring U.S. IaaS providers to submit to the Department a report when a foreign person transacts with the IaaS provider to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity. The report, at a minimum, must include the identity of the foreign person and the existence of a training run that meets the criteria set forth in this section, as well as any other information specified in regulation. This section of E.O. 14110 also instructs the Secretary to determine the set of technical conditions that a large AI model must possess in order to have the potential capabilities that could be used in malicious cyber-enabled activity and to update that determination as necessary and appropriate.

Section 4.2(c) of this E.O. also requires that U.S. IaaS providers prohibit any foreign reseller of their U.S. IaaS product from providing those products unless such foreign reseller submits to the U.S. IaaS provider a report, which the U.S. IaaS provider must provide to the Department, detailing each instance in which a foreign person transacts with the foreign reseller to use the U.S. IaaS product to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity. In accordance with this requirement, section 4.2(d) requires the proposed regulations to require U.S. IaaS providers to ensure that foreign resellers of U.S. IaaS products verify the identity of any foreign person that obtains an IaaS account from the foreign resellers. The Department is directed to set forth the minimum standards that a U.S. IaaS provider must require of their foreign resellers to verify the identity of a foreign person who opens an account or maintains an existing account with a foreign reseller.

III. Comments on the Advanced Notice of Proposed Rulemaking

On September 24, 2021, the Department published in the **Federal Register** an advanced notice of proposed rulemaking (ANPRM), 86 FR 53018 (Sep. 24, 2021), soliciting comments on how the Department should implement various provisions of sections 1 and 2 of E.O. 13984, described above, and section 5 of E.O. 13894, which defines several key terms as they relate to the proposed regulations. The Department received twenty-one (21) comments to the ANPRM, which are available on the public rulemaking docket at *https://www.regulations.gov.*

This section summarizes the comments received in response to the ANPRM and explains the Department's proposed regulations to implement sections 1, 2, and 5 of E.O. 13984. The proposed rule text incorporates many of the suggestions the Department received in response to the ANPRM, as set out in more detail below.

(1) Definitions

The Department sought comments on the terms ''United States person'' and ''United States Infrastructure as a Service Provider.'' The commenters who responded to this question argued that the term ''United States person'' should not be interpreted to include foreign subsidiaries of a U.S. IaaS provider, as this extension would exceed the scope of E.O. 13984. Commenters differed about how broadly to interpret the term ''United States Infrastructure as a Service Provider.'' Many requested the Department to interpret this term as broadly as possible to capture as much potential foreign malicious cyber activity as possible. Others believed the Department should interpret the definition narrowly to avoid implicating cloud service providers who offer other cloud-based services, such as Platform as a Service (PaaS) and Software as a Service (SaaS) offerings, but do not offer IaaS products. This proposed rule reflects the Department's consideration of all relevant comments.

(2) Customer Identification Program Regulations and Relevant Exemptions

In the ANPRM, the Department sought information about how to implement requirements for companies to verify a foreign person's identity upon the opening of an Account and while maintaining an existing Account. The Department sought comments on verification procedures and recordkeeping requirements the Department should consider including in regulations.

Many commenters expressed support for implementing data retention and recordkeeping requirements, as directed by E.O. 13984, across a broad spectrum of U.S. IaaS providers' products or services to capture a large portion of malicious cyber-enabled activity on these platforms. While commenters generally supported requiring U.S. IaaS providers to verify the identity of all prospective customers, some suggested that any regulation the Department promulgates in response to E.O. 13984 will be ineffective, as malicious cyber actors are savvy enough to avoid identity verification.

Other commenters requested that the Department's proposed regulations allow U.S. IaaS providers to adopt risk-based approaches to verify the identity of their customers. These approaches, they argued, would allow IaaS providers flexibility to adjust their CIPs to meet new threats and vulnerabilities as they arise. Most commenters agreed that the Department should consider the costs and benefits of these requirements for U.S. IaaS providers and expressed concern that the costs of compliance would be substantial. As discussed further below, the Department has proposed standards and procedures that take into consideration the size, complexity, and risk profile of the IaaS provider and its product offerings.

The Department requested comments on current practices, if any, that U.S. IaaS providers use to verify the identity of their customers and the burden that any new regulations would impose on these IaaS providers. Commenters reported that there is no uniform set of data that U.S. IaaS providers collect before opening an Account for a customer, but email addresses and payment methods are normally required. Most commenters indicated that any requirements in this proposed regulation would impose burdens on U.S. IaaS providers, and that the Department should weigh this burden against the anticipated benefit any regulations mandating identity verification would have on national security. The Department acknowledges that this rulemaking will impose compliance costs for at least some U.S. IaaS providers and has addressed these costs in the regulatory impact analysis included in the preamble of this proposed rule.

The Department asked about the impact any proposed regulations would have on data protection and security, especially considering the European Union General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Many commenters encouraged the Department to propose regulations that would enable U.S. law enforcement officials to gain access to data stored by domain name registries and registrars that has proven more difficult since the enactment of the GDPR. Others focused on ensuring that the processing of customers' data to carry out the provisions of any proposed regulation would be consistent with the GDPR or CCPA. Still others requested that any proposed regulation not frustrate ongoing negotiations to open the flow of data between foreign countries and the United States. The Department acknowledges these comments and has sought to ensure these proposed regulations are consistent with national and international obligations, either because the specific information requested is not protected, or because the need for data collection falls into relevant exemptions.

The Department sought comments on how to implement the authority, granted by section 1(c) of E.O. 13984, to provide exemptions from the requirements of any regulations issued pursuant to E.O. 13894. Many commenters expressed hope that the Department could promulgate best practices for IaaS providers to adopt or strive to meet in order to avoid compliance costs associated with any proposed regulations. Others asked the Department to tailor these regulations to apply only to those products and services most used by foreign malicious cyber actors. The Department is proposing procedures for IaaS providers to obtain exemptions from the CIP requirements. Under these procedures, a U.S. IaaS provider seeking to obtain an exemption for itself, a specific type of account or lessee, or its foreign reseller, would provide a written submission to the Secretary outlining its program to comply with security best practices to deter the abuse of U.S. IaaS products. A finding by the Secretary that the program incorporates such best practices would exempt an IaaS provider from the CIP requirements in section 1(a) of E.O. 13984.

Some commenters urged the Department not to include exemptions, believing this practice to be contrary to the intent of E.O. 13984 to address the use of U.S. IaaS products for malicious cyber-enabled activities. In these proposed regulations, the Department has endeavored to provide a pathway to enable U.S. IaaS providers to apply for an exemption where such exemption is warranted while still accomplishing the policy goals of E.O. 13984. The Department welcomes comments and feedback on its proposed approach, as well as on potential standards and best practices that could deter the abuse of U.S. IaaS products by malicious actors.

(3) Special Measures Restrictions

In the ANPRM, the Department sought comments on procedures the Secretary should use to decide when and how to impose a special measure. The Department asked what sources of information the Secretary should consider, how the Secretary should publish any findings, how long the special measure's effects should last, and how to determine which special measure to invoke.

Commenters encouraged the Department to consider how to leverage existing authorities and procedures, such as the Department's existing authority to prohibit certain Information and Communications Technology and Services (ICTS) transactions or the Department of the Treasury's Office of Foreign Assets Control's (OFAC) sanctions procedures, to minimize the burden of these special measures. Other commenters indicated that the threat of these special measures will result in lost U.S. business, as foreign persons may move to IaaS products and services furnished from companies headquartered in foreign countries. Still others expressed doubt that these special measures would accomplish their intended purpose.

In crafting these proposed regulations regarding special measures, the Department looked to a variety of sources, including OFAC's sanction procedures, and has sought to minimize the costs to U.S. businesses while still meeting the requirements of E.O. 13984.

IV. Proposed Rule and Request for Comments

Following consideration of the comments received in response to the ANPRM, the Department is proposing regulations to implement sections 1, 2, and 5 of E.O. 13984 and the applicable provisions of E.O. 14110. The provisions implementing E.O. 13984 would apply to U.S. IaaS providers that offer U.S. IaaS products, as defined in E.O. 13984 and this proposed rule. ''U.S. IaaS providers'' includes any U.S. person that offers IaaS products, to include both direct providers of U.S. IaaS products and any of their U.S. resellers.

To implement section 1 of E.O. 13984, the Department proposes to require providers to verify the identity of foreign customers. To implement section 2 of E.O. 13984, the Department proposes procedures for the Secretary's decision-making process regarding whether and how to issue determinations about special measures. Regarding the definitions in section 5 of E.O. 13984, the Department proposes interpretations of terms defined in the E.O. and proposes definitions for several additional key terms.

To implement section 4.2(c) of E.O. 14110, the Department proposes regulations related to foreign resellers of U.S. IaaS products that would apply to U.S. IaaS providers as defined in E.O. 13984 and this proposed rule. The Department uses ''foreign reseller'' to mean any foreign person who has established an account with a U.S. IaaS provider to provide IaaS products

subsequently, in whole or in part, to a third party.

To implement section 4.2(c) of this E.O., the Department proposes a process for U.S IaaS providers to report to the Department when they have knowledge they will engage or have engaged in a transaction with a foreign person that could allow that foreign person to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity. To implement section 4.2(d) of this E.O., the Department proposes regulations that would require U.S. IaaS providers to require foreign resellers of their U.S. IaaS products to verify the identity of foreign persons who open or maintain an account with a foreign reseller.

The Department proposes definitions for terms used within E.O. 14110, including a definition for a ''large AI model with potential capabilities that could be used in malicious cyber-enabled activity.'' Based on this definition, the Secretary will determine, as required by E.O. 14110, the set of technical conditions that a large AI model must possess in order to have the potential capabilities that could be used in malicious cyber-enabled activity. That determination will be a binding interpretation of what constitutes a ''large AI model with potential capabilities that could be used in malicious cyber-enabled activity.'' As this area of technology is fast developing, and as directed by E.O. 14110, the Secretary will update, as ''necessary and appropriate,'' the initial determination of which set of technical conditions meet the definition. The Department will publish these binding updates to the technical condition determinations in the **Federal Register**. The Department requests comments on all aspects of this proposed rule.

(1) Definitions

This proposed rule adopts several definitions found in section 5 of E.O. 13984, including ''entity,'' ''foreign jurisdiction,'' ''foreign person,'' ''Infrastructure as a Service Account,'' ''Infrastructure as a Service product,'' ''Malicious cyber-enabled activities,'' ''person,'' ''Reseller Account,'' ''United States person,'' and ''U.S. Infrastructure as a Service product.'' In addition, this proposed rule clarifies the definition of ''U.S. Infrastructure as a Service provider'' found in section 5 of E.O. 13984. The proposed rule also adopts several definitions found in section 3 of E.O. 14110, including ''artificial intelligence'' or ''AI,'' ''AI model,'' ''AI system,'' ''dual-use foundation model,'' ''foreign reseller,'' ''generative AI,'' ''integer operation,'' ''machine learning,'' and ''model weight.'' Finally, the Department proposes several definitions of key terms in this rule, including ''customer'' and ''beneficial owner,'' as well as definitions for terms such as ''availability,'' ''confidentiality,'' ''Customer Identification Program,'' ''Department,'' ''disassociability,'' ''foreign beneficial owner,'' ''foreign customer,'' ''foreign reseller, ''individual,'' ''integrity,'' ''knowledge,'' ''large AI model with potential capabilities that could be used in malicious cyber-enabled activity,'' ''manageability,'' ''predictability,'' ''privacy-preserving data sharing and analytics,'' ''Red Flag,'' ''reseller,'' ''risk-based,'' ''Secretary,'' ''threat landscape,'' ''training,'' ''training run,'' and ''United States reseller.'' Some of the proposed definitions are discussed below, although the Department welcomes comments on all definitions in this proposed rule.

A. Availability

The Department proposes to define ''availability'' as ensuring timely and reliable access to and use of information and information systems by an authorized person or system, including resources provided as part of a product or service.

B. Beneficial Owner

E.O. 13984 requires verification of the identity of foreign persons that obtain accounts, and it defines ''person'' as ''an individual or entity.'' Therefore, the Department proposes to require U.S. IaaS providers to collect the same identifying information and verify the identity of beneficial owners of Accounts owned or maintained by entities. Under the proposed rule, a beneficial owner is defined as an individual who either: (1) exercises substantial control over a Customer, or (2) owns or controls at least 25 percent of the ownership interests of a Customer. The Department seeks comments on these definitions, including the meaning of ''substantial control.''

C. Confidentiality

The Department proposes to define ''confidentiality'' as preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

D. Customer Identification Program

The Department proposes to define ''Customer Identification Program'' as a program created by a U.S. IaaS provider or foreign reseller that dictates how the IaaS provider will collect identifying information about its customers, how the IaaS provider will verify the identity of its foreign customers, store and maintain identifying information, and notify its customers about the disclosure of identifying information.

E. Department

The Department proposes to define ''Department'' as the United States Department of Commerce.

F. Disassociability

The Department proposes to define ''disassociability'' as enabling the processing of data or events without association to individuals or devices beyond the operational requirements of the system.

G. Foreign Beneficial Owner

The Department proposes to define ''foreign beneficial owner'' as a beneficial owner that is not a United States person.

H. Foreign Customer

The Department proposes to define ''foreign customer'' as a customer that is not a United States person.

I. Foreign Reseller

The Department proposes to adopt the definition from E.O. 14110 and define ''foreign reseller'' to mean a foreign person who has established an IaaS Account to provide IaaS subsequently, in whole or in part, to a third party. This is consistent with the definition for foreign reseller included in E.O. 14110.

J. Individual

The Department proposes to define ''individual'' as any natural person.

K. Infrastructure as a Service Product

This proposed definition adopts the E.O. 13984 definition for ''Infrastructure as a Service product'', which is any product or service offered to a consumer, including complimentary or ''trial'' offerings, that provides processing, storage, networks, or other fundamental computing resources, and with which the consumer is able to deploy and run software that is not predefined, including operating systems and applications. The consumer typically does not manage or control most of the underlying hardware but has control over the operating systems, storage, and any deployed applications. The term is inclusive of ''managed'' products or services, in which the provider is responsible for some aspects of system configuration or maintenance, and ''unmanaged'' products or services, in which the provider is only responsible for ensuring that the

product is available to the consumer. The term is also inclusive of ''virtualized'' products and services, in which the computing resources of a physical machine are split between virtualized computers accessible over the internet (*e.g.,* ''virtual private servers''), and ''dedicated'' products or services in which the total computing resources of a physical machine are provided to a single person (*e.g.,* ''baremetal'' servers).

The Department believes that this expansive definition will allow for regulations to apply to a broad range of IaaS product offerings that can be used by foreign malicious cyber actors to carry out attacks on the United States or United States persons. Note that this definition includes all service offerings for which a consumer does not manage or control the underlying hardware, but rather contracts with a third party to provide access to this hardware. This definition would capture services such as content delivery networks, proxy services, and domain name resolution services. It does not, however, capture domain name registration services for which a consumer registers a specific domain name with a third party, as that third party does not provide any processing, storage, network, or other fundamental computing resource to the consumer. The Department seeks comment on the categories of products or services that fall within this definition.

L. Integrity

The Department proposes to define ''integrity'' as guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.

M. Knowledge

The Department proposes to define ''knowledge'' as knowledge of a circumstance (the term may be a variant, such as ''know,'' ''reason to know,'' or ''reason to believe'') including not only positive knowledge that the circumstance exists or is substantially certain to occur, but also an awareness of a high probability of its existence or future occurrence. Such awareness is inferred from evidence of the conscious disregard of facts known to a person and is also inferred from a person's willful avoidance of facts. This definition is similar to that in the Department's Export Administration Regulations.

N. Large AI Model With Potential Capabilities That Could Be Used in Malicious Cyber-Enabled Activity

The Department proposes to define ''large AI model with potential capabilities that could be used in malicious cyber-enabled activity'' as any AI model with the technical conditions of a dual-use foundation model, or that otherwise has technical parameters of concern, that has capabilities that could be used to aid or automate aspects of malicious cyber-enabled activity, including but not limited to social engineering attacks, vulnerability discovery, denial-of-service attacks, data poisoning, target selection and prioritization, disinformation or misinformation generation and/or propagation, and remote command-and-control, as necessary and appropriate of cyber operations. The Department seeks comment on this proposed definition.

E.O. 14110 also instructs the Secretary to determine and to update, ''as necessary and appropriate,'' the set of technical conditions for a ''large AI model to have potential capabilities that could be used in malicious cyber-enabled activity.'' Based on the above definition, the Secretary will make this initial determination and any necessary and appropriate updates to it which the Department will publish in the **Federal Register**. Such technical conditions may include the compute used to pre-train the model exceeding a specified quantity.

The Department seeks comment on the proposed definition, as well as on the Secretarial process for determining and, because of rapidly advancing technology, updating the set of specific technical conditions necessary for a large AI model to meet the definition and have the potential capabilities that could be used in malicious cyber-enabled activities.

O. Manageability

The Department proposes to define ''manageability'' as providing the capability for granular administration of data, including alteration, deletion, and selective disclosure.

P. Predictability

The Department proposes to define ''predictability'' as enabling reliable assumptions by individuals, owners, and operators about data and their processing by a system, product, or service.

Q. Privacy-Preserving Data Sharing and Analytics

The Department proposes to define ''privacy-preserving data sharing and analytics'' as the use of privacy-enhancing technologies to achieve disassociability, predictability, manageability, and confidentiality when performing analytics on data.

R. Red Flag

The Department proposes to define ''Red Flag'' as a pattern, practice, or specific activity that indicates the possible existence of malicious cyber-enabled activities.

S. Reseller

The Department proposes to define ''reseller'' as a person that maintains a Reseller Account.

T. Risk-Based

The Department proposes to define ''risk-based'' as based on an assessment of the relevant risks, including those presented by the various types of service offerings maintained by an IaaS provider, the methods used to open an Account, the varying types of identifying information available to an IaaS provider, and an IaaS provider's customer base.

U. Secretary

The Department proposes to define ''Secretary'' as the Secretary of Commerce or the Secretary's designee.

V. Threat Landscape

The Department proposes to define ''threat landscape'' as the broad environment of geopolitical, economic, and technological factors that must be evaluated when developing risk-based procedures that enable an IaaS provider to form a reasonable belief of the true identity of each Account owner and beneficial owner to deter facilitating significant malicious cyber-enabled activities.

W. Training or Training Run

The Department proposes to define ''training'' or ''training run'' as any process by which an AI model learns from data through the use of computing power.

X. United States Infrastructure as a Service Product

The Department proposes to clarify the E.O.'s definition of ''United States Infrastructure as a Service product.'' The E.O. defines this term as ''any Infrastructure as a Service Product owned by any United States person or operated within the territory of the United States of America.'' The Department considers Reseller Accounts as IaaS products.

Y. United States Infrastructure as a Service Provider

E.O. 13984 defines ''United States Infrastructure as a Service provider'' as ''any United States Person that offers any Infrastructure as a Service product.'' The Department notes that this

definition of ''United States Infrastructure as a Service provider'' includes any United States person that is a direct provider of U.S. IaaS products and any of their U.S. resellers. The Department proposes to consider U.S. resellers of U.S. IaaS products as IaaS providers subject to these proposed regulations.

In response to the ANPRM, several commenters suggested that the Department clarify whether this term includes foreign subsidiaries of United States persons. Specifically, these commenters believed including foreign subsidiaries of United States persons in this definition would exceed the scope of the E.O., which focuses on threats to the United States from U.S. IaaS products, not those offered by foreign subsidiaries. The Department proposes to clarify that a foreign subsidiary of a U.S. IaaS provider is not considered to be a ''United States Infrastructure as a Service provider.''

E.O. 13984 requires the Secretary to propose regulations to require providers to ''verify the identity of a foreign person in connection with the opening of an Account or the maintenance of an existing Account.'' It requires that any regulations set out the types of documentation or procedures ''required to verify the identity of any foreign person acting as a lessee or sub-lessee of these products or services.'' The Department proposes to consider U.S. resellers of U.S. IaaS products as U.S. IaaS providers subject to these proposed regulations.

(2) Customer Identification Program Regulations and Relevant Exemptions

Under this proposed rule, U.S. IaaS providers and their foreign resellers would maintain CIPs, perform effective customer verification, and maintain identifying information about their foreign customers, which is critical to combating malicious cyber-enabled activities. The Department proposes to 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. The Department will consider allowing U.S. IaaS providers an adjustment period to implement some provisions of this proposed regulation and notify the Department accordingly, and anticipates that compliance would be required within one year of the date of publication of any final rule.

Accordingly, the Department proposes to require IaaS providers develop their own risk-based CIP. Taking into consideration the different types of IaaS Accounts, the different methods used to open the Accounts, and the types of information available to identify foreign malicious cyber actors, while avoiding the imposition of an undue burden on providers, the Department proposes to allow each provider to create a CIP that matches its unique service offerings and customer bases. Provided that IaaS providers meet certain minimum requirements in their CIPs, providers can create CIPs that are flexible and minimally burdensome to their business operations.

The Department proposes to require U.S. resellers of U.S. IaaS Accounts to establish CIPs and identity verification procedures to be used any time they act as a reseller for U.S. IaaS products. The CIPs of such U.S. resellers would be subject to the minimum standards in this proposed rule. U.S. resellers would be responsible for establishing the identity of their potential customers, including all prospective beneficial owners of these Accounts, and determining whether they are U.S. persons. U.S. resellers would also be responsible for verifying the identity of their foreign customers under this proposed rule. The Department requests comments on whether resellers that are small businesses might find it more difficult to develop a CIP. The Department proposes 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 Department further seeks comments on whether resellers currently request identifying information from their customers and how these resellers verify the identity of their prospective foreign customers.

The Department seeks comments on whether to require IaaS providers to conduct third-party or internal audits to confirm their compliance with CIP requirements in the proposed rule. The Department also seeks comments on whether the Department should receive and approve all CIPs. The Department additionally seeks comments on whether the rulemaking should require U.S. IaaS providers to submit Red Flags either to the Department or to another relevant department or agency. Below, the Department explains additional specific requirements for CIPs.

A. Data Collection Requirements

Under the proposed rule, each CIP must include procedures that U.S. IaaS providers and their foreign resellers will use to collect information from all covered existing and prospective customers, that is, those who have applied for an account. At a minimum, the following data would be collected: a customer's name, address, the means and source of payment for each customer's Account, email addresses and telephone numbers, and internet protocol (IP) addresses used for access or administration of the Account. IaaS providers may alter their CIPs to require additional information from prospective customers that is necessary to verify the identity of any foreign person, but all CIPs must, at a minimum, collect the previously listed data. The Department proposes omitting a requirement for collecting and verifying national identification numbers because, based on public feedback, the Department believes that national identification number verification would be unduly burdensome and would not be necessary to verify identity. The Department seeks comments on whether other forms of identification, such as digital or technology-based identification, should be included as an acceptable means by which IaaS providers may verify customers' identities, and if companies have privacy-protecting or privacy-enhancing technologies to verify this same information or other alternatives that can effectively achieve identity verification.

The Department believes that many U.S. IaaS providers and their foreign resellers already collect this information from their customers, and that the proposed rule would set a baseline for data collection that would help all providers effectively verify and document the identities of their customers. The Department seeks comments on the costs and burdens associated with this proposed requirement and whether the Department should include additional data collection in a baseline requirement for CIPs. The Department proposes a requirement that providers make a written description of their CIPs available for inspection by the Department, which may identify specific shortcomings for providers to resolve. The Department seeks comment on this proposal.

The Department is proposing to require that CIPs account for the collection of identifying information about the actual Account owner and all beneficial owners of the Account. Specifically, the proposed required description of the CIP would specify how providers would ensure that all beneficial owners of an Account at its inception and any new beneficial owner added to the Account undergo the same identification procedures as the person opening the Account. The Department seeks comment on this approach.

B. Prospective Customers From the United States

E.O. 13984 addresses threats to U.S. IaaS products and services by foreign malicious cyber actors. Section 1 of the E.O. therefore requires the Department to propose regulations to require U.S. IaaS providers to verify the identity of ''a foreign person that obtains an Account.''

Therefore, the Department proposes to require U.S. IaaS providers to verify the identity of foreign persons who obtain an Account from providers and to require the same of their foreign resellers. Although providers would be required to create a CIP that includes the minimum data collection requirements for all prospective customers, they would not be required to verify the identity of customers with Accounts opened by or on behalf of a U.S. person, unless a foreign beneficial owner is added to the Account or the Account or a portion of the Account is resold to a foreign person.

The Department seeks comments about whether the proposed data collection requirements above would enable providers to accurately distinguish foreign current and prospective customers from others. If these proposed requirements are inadequate, what additional required information should be included in the CIPs to aid in these efforts? The Department also seeks comments on the availability of secure data deletion standards and whether to require their implementation for Accounts determined to be opened, owned, and accessible exclusively by U.S. persons.

C. Identity Verification

The Department proposes to require that CIPs include procedures to ensure that U.S. IaaS providers and their foreign resellers verify the identity of all foreign Account owners and foreign beneficial owners. Under the proposed rule, providers may craft their own procedures and methods to verify the identity of their prospective foreign customers and beneficial owners, provided that their CIPs include risk-based procedures that enable the provider to form a reasonable belief about the true identity of each customer and beneficial owner. These procedures must be based on a provider's assessment of the relevant risks, including those presented by the various types of service offerings maintained by the provider, the methods used to open an Account, the varying types of identifying information available to the provider, and the provider's customer base. Under the proposed rule, the CIP must establish whether a provider will use documentary or non-documentary verification or a combination of both. It must establish how a provider will verify the identity of its customers when the customer is unable to produce the requested documents. The Department believes this flexibility would minimize the burden placed on providers by these regulations. The Department seeks comments on this risk-based approach to allow providers to form reasonable beliefs of the true identity of each customer and beneficial owner and on what information they would need to collect to accomplish this.

Under the proposed rule, the CIP must include steps a provider would take if it is unable to verify the identity of any customer, including refusing to open an Account and/or additional monitoring pending attempts at verification. It must further set out the terms under which a customer may continue to have access to an Account while the provider attempts to verify the identity of the customer, and when a provider would close an Account after attempts to verify a customer's identity have failed. Additionally, it must describe measures for redress and issue management to address situations in which legitimate customers may fail identity verification, or in which their information was compromised and a fraudulent account established. The Department seeks comments on whether to require specific verification methods, such as email or payment verification, for all prospective customers. The Department seeks comments on whether the Department should allow providers to grant potential customers access to Accounts prior to successful identity verification. The Department seeks comments on whether including reference to National Institute of Standards and Technology (NIST) Special Publication (SP) 800–63 regarding digital identity guidelines would help IaaS providers meet requirements for identity verification.

D. Recordkeeping

The Department proposes to require U.S. IaaS provider and foreign reseller of U.S. IaaS product CIPs to include procedures for maintaining, protecting, and obtaining access to records of relevant customer information accessed in the process of verifying customer identities. At a minimum, this record must include a description of the identity evidence and attributes provided by the customer when the customer first attempted to open an Account, a description of the methods and results of any measures undertaken to verify customer identity, and a description of the resolution of any substantive discrepancy discovered when verifying the identifying information. The proposed rule leaves to IaaS providers the discretion to design their own recordkeeping procedures, so long as these procedures obtain this minimum information.

The Department proposes to require that CIPs of U.S. IaaS providers and their foreign reseller include requirements to securely maintain these records and describe measures taken to ensure that the information is secure. The proposed regulations would require that IaaS providers limit access to any records or documents created, retained, or accessed pursuant to these regulations by any third parties or IaaS provider employees without a need-to-know basis for obtaining this access. However, no such requirement should be read to limit IaaS providers' ability to share security best practices and threat information with other IaaS providers, relevant consortia, or the U.S. Government as needed and consistent with applicable law. The Department seeks comments on the feasibility of this approach and the costs of doing so. The Department further seeks comments on whether there currently exist best practices for the maintenance, storage, and security of customer identifying information.

The Department proposes to require that U.S. IaaS providers retain these records for a period of two years after the date upon which an Account was last accessed or closed. The Department preliminarily determines that a two-year period is necessary to allow law enforcement the ability to gain access to this information should an Account be suspected of hosting malicious cyber-enabled activity. The Department seeks comments on the burdens to IaaS providers of maintaining these records for two years, and whether there are alternative ways to allow for both immediate and long-term access to customer information should an Account be used for malicious cyber-enabled activity. The Department seeks comments on whether to require that CIPs include procedures to address situations where an Account that has been inactive for more than two years is subsequently accessed by a foreign person, and whether to require that IaaS providers request that the foreign person provide the enumerated identifying information again in these circumstances.

E. Ensuring Verification for Foreign Resellers

As directed in E.O. 14110, the Department proposes to require that U.S IaaS providers only initiate or continue a reseller relationship with foreign resellers of U.S. IaaS products that maintain and implement a CIP that meets the requirements for CIPs of U.S. IaaS providers in this proposed rule. The Department recognizes that it will take U.S. IaaS providers time to educate, coordinate, and collect information from their foreign resellers on CIP requirements and therefore anticipates allowing U.S. IaaS providers up to one year to implement such final provisions and notify the Department accordingly. Under this proposed rule, U.S. IaaS providers would be required to furnish a copy of any foreign reseller's CIP to the Department within ten calendar days following a request for the same from the Department. The Department seeks comments on the potential challenges that U.S. IaaS providers would face when collecting this information from their foreign resellers of U.S. IaaS products. The proposed rule would also require that, upon receipt of evidence that indicates the failure of a foreign reseller to maintain or implement a CIP or that indicates malicious cyber-enabled activity, U.S. IaaS providers must report malicious cyber-enabled activity and close accounts associated with the activity and must terminate the reseller relationship within 30 calendar days. The Department seeks comments on the challenges U.S. IaaS providers would face in investigating and remediating malicious cyber activity by foreign resellers, as well as the contractual difficulties posed by terminating the relationship with a non-compliant foreign reseller. The Department further seeks comments on the extent to which there currently exist customer identification and verification practices which U.S. IaaS providers require their foreign resellers to use.

F. Customer Identification Program Updates and Certifications

The Department proposes to require that U.S. IaaS providers submit to the Department certain information about their CIPs and their foreign resellers' CIPs, to include procedures on verifying customer identity and detecting malicious cyber activity, as well as information and data on their provision of IaaS products. The Department further proposes to require that U.S. IaaS providers and their foreign resellers update their CIPs annually to protect against new cyber threats and vulnerabilities, as well as to increase efficiency and data security, and to certify to the Department that such annual updates have occurred. The Department proposes that U.S. IaaS providers must notify the Department of any updates to their CIP or any CIP of their foreign resellers. In these annual certifications, providers would also attest to the Department that, since the date of last certification, they have reviewed their CIPs and updated their CIPs to account for any changes in their service offerings and for changes to the threat landscape. The certification would include an attestation that the current CIP complies with the provisions of the proposed rule. This attestation would require the provider to indicate the frequency with which it was unable to verify the identity of a foreign customer in the prior calendar year and record the resolution for each of those situations. The Department seeks comments on the usefulness and feasibility of such attestation and whether the Department should require additional information in these certifications, the procedures for submission of such certifications, and whether the Department should require these certifications more or less frequently than annually. The Department seeks comments on whether there currently exist best practices for customer identification and verification that providers can use as a model for their CIPs.

G. Exemptions

Section 1(c) of E.O. 13984 permits the Secretary, in accordance with such standards and procedures as the Secretary may delineate and, in consultation with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, to exempt any U.S. IaaS provider, or any specific type of Account or lessee, from the requirements of any regulation issued pursuant to the section. Such standards and procedures may include a finding by the Secretary that a provider, Account, or lessee complies with security best practices to otherwise deter abuse of IaaS products. Section 4.2(d)(iii) of E.O. 14110 also provides that the Secretary may ''exempt a United States IaaS Provider with respect to any specific foreign reseller of their United States IaaS Products, or with respect to any specific type of account or lessee, from the requirements of any regulation issued pursuant to this subsection,'' that section being related to CIP requirements for foreign resellers of U.S. IaaS products.

This NPRM proposes standards and procedures for exemptions from CIP requirements in §§ 7.302 through 7.305 for U.S. IaaS providers and with regard to any of their specific foreign resellers. The regulations propose that providers seeking an exemption submit a written request electronically. The Department anticipates that the final rule would designate an email address to receive such requests. The Department seeks comments on these standards and procedures in proposed § 7.306. The Department seeks comment on whether there exist security best practices to deter abuse of U.S. IaaS products that the Secretary may reference in the future to authorize exemptions from these regulations, including but not limited to improving event log management to generate, safeguard, and retain logs of IaaS providers' system and network events, both to improve incident detection and to aid in incident response and recovery activities. The Department also seeks comments on whether there are appropriate safe harbor activities that might form the basis of an exemption program.

(3) Special Measures Regulations

A. Special Measures Requirements

The Department proposes regulations to implement the authority provided to the Secretary to take either of the special measures enumerated in E.O. 13984, should the Secretary determine that reasonable grounds exist for concluding that a jurisdiction or person outside of the U.S. ''has any significant number of foreign persons offering U.S. IaaS products that are used for malicious cyber-enabled activities or any significant number of foreign persons directly obtaining U.S. IaaS products for use in malicious cyber-enabled activities.'' The Department proposes to allow the Department to initiate investigations of its own accord or accept referrals from other executive branch agencies or providers to evaluate evidence about a particular foreign jurisdiction or person to determine whether to impose a special measure. The Department would then assess the information in its possession and information available from public and other sources about a foreign person or foreign jurisdiction to determine whether imposing a special measure would be appropriate. Should the Secretary determine that the evidence warrants the imposition of a special measure, the Secretary would issue a determination in the **Federal Register**, to take effect 30 days after publication, that would set out the reasonable grounds for this determination and

would indicate which special measure the Secretary would intend to use.

B. Reasonable Grounds Determination

E.O. 13984 provides that, when determining whether a particular foreign jurisdiction ''has any significant number of foreign persons offering U.S. IaaS products that are used for malicious cyber-enabled activities or any significant number of foreign persons directly obtaining U.S. IaaS products for use in malicious cyber-enabled activities,'' the Secretary must consider, among other relevant information: (1) evidence that foreign malicious cyber actors have obtained U.S. IaaS products in that foreign jurisdiction, including whether such actors obtained such U.S. IaaS products through reseller accounts; (2) the extent to which that foreign jurisdiction is a source of malicious cyber-enabled activities; and (3) whether the U.S. has a mutual legal assistance treaty with that foreign jurisdiction, and the experience of U.S. law enforcement officials in obtaining information about activities involving U.S. IaaS products originating in or routed through such foreign jurisdiction.

With respect to foreign persons, the Secretary must assess: (1) the extent to which a foreign person uses U.S. IaaS products to conduct, facilitate, or promote malicious cyber-enabled activities; (2) the extent to which U.S. IaaS products offered by a foreign person are used to facilitate or promote malicious cyber-enabled activities; (3) the extent to which U.S. IaaS products offered by a foreign person are used for legitimate business purposes in the jurisdiction; and (4) the extent to which actions short of the imposition on special measures are sufficient, with respect to transactions involving the foreign person offering U.S. IaaS products, to guard against malicious cyber-enabled activities. Finally, the Secretary may analyze any information gleaned through the Department's existing authority to review ICTS transactions pursuant to its authority derived from Executive Order 13873 of May 17, 2019, ''Securing the Information and Communications Technology and Services Supply Chains'' (84 FR 22689). The Department seeks comments on any additional relevant factors the Secretary should consider.

C. Choosing a Special Measure

The Department proposes to require that the Secretary's investigation process include consultation with the agencies referenced in E.O. 13984, namely the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of National Intelligence, and other heads of other executive departments and agencies as the Secretary deems appropriate, to determine which special measure to impose. This consultation would include a review of the available evidence to determine whether to impose a special measure against a foreign jurisdiction or against a foreign person; a consideration of whether the imposition of the special measure would create a significant competitive disadvantage, including any undue cost or burden associated with compliance, for providers; and a determination of the extent to which the imposition of a special measure or the timing of the special measure would have a significant adverse effect on legitimate business activities involving the foreign jurisdiction or foreign person. Finally, the determination would include an assessment of the effect of any special measure on U.S. supply chains, public health or safety, national security, law enforcement investigations, or foreign policy. The Department seeks comments on whether additional considerations should be included before the Secretary would choose a special measure.

(3) AI Training Reporting Requirements

Section 4.2 (c)(i) of E.O. 14110 instructs the Secretary to ''propose regulations that require United States IaaS Providers to submit a report to the Secretary of Commerce when a foreign person transacts with that United States IaaS provider to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity.'' Such report shall include, at a minimum, the identity of the foreign person and the existence of any training run of an AI model meeting the criteria set forth in E.O. 14110 or otherwise determined by the Secretary, and other information as identified by the Secretary. In addition, section 4.2(c)(ii) of E.O. 14110 directs that U.S. IaaS providers must be required to prohibit foreign resellers of their U.S. IaaS products from providing those products unless the foreign resellers submit such reports to the provider, which the provider must provide to the Secretary.

This proposed rule would require such providers to report to the Department information on instances of training runs by foreign persons for large AI models with potential capabilities that could be used in malicious cyber-enabled activity. Reportable information includes the identifying information about the training run (*i.e.,* the customer's name, address, the means and source of payment for the customer's Account, email addresses, telephone numbers, and IP addresses) and the existence of the training run. The Department requests comment on what additional information, if any, the Department should require providers report.

Section 4.2(c)(iii) instructs the Secretary to ''determine the set of technical conditions for a large AI model to have potential capabilities that could be used in malicious cyber-enabled activity, and revise that determination as necessary.''

The Department has proposed that a model meets the definition of a ''large AI model with potential capabilities that could be used in malicious cyber-enabled activity'' if it meets technical conditions issued by the Department in interpretive rules published in the **Federal Register**. The Department will update the technical conditions, based on technological advancements, as necessary and appropriate, as directed by E.O. 14110, through interpretive rules published in the **Federal Register**. The Department seeks comment on the definition of a ''large AI model that could be used in malicious cyber-enabled activity,'' and on what Red Flags, if any, the Department should adopt that would create a presumption that a foreign person is training a model with the technical conditions set out in E.O. 14110.

(4) Compliance and Enforcement

Though issued pursuant to the President's authority derived from IEEPA, E.O. 13984 is silent as to penalties for noncompliance. The Department proposes to clarify that any person who commits a violation of this proposed rule, if finalized, may be liable to the United States for civil or criminal penalties under IEEPA. Although the Department currently has penalty provisions under 15 CFR 7.200 for violations of Final Determinations issued pursuant to the Department's ICTS authorities pursuant to the IEEPA, the Department believes it is important to have a new enforcement section specific to violations of these IaaS-related provisions. Accordingly, the Department is adding a section on enforcement, which lists civil and criminal penalties, and the acts particular to these IaaS-related provisions that will result in those penalties. For example, the new enforcement section specifies that it is a violation to fail to create a CIP, or to fail to file with the Department a CIP certification, or fail to seek reauthorization for such CIPs on an

annual basis. It is also a violation to fail to inform the Department about a covered IaaS transaction that might result in a customer obtaining or using a large AI model with potential capabilities that could be used in malicious cyber-enabled activity when an IaaS provider knows or should know of such transaction.

Regarding penalties for violations, whether a violation results in a civil or criminal penalty will depend largely on the nature of the offense. For example, intentionally or knowingly violating a provision of these regulations could result in criminal penalties, while unintentional violations are more likely to result in civil penalties. The Department seeks comments on this approach.

V. Classification

a. Executive Order 12866

This rulemaking has been determined to be a significant action under Executive Order 12866, as amended by Executive Order 14094.

b. Regulatory Impact Analysis

As required by Executive Order 12866, and the Regulatory Flexibility Act, 5 U.S.C. 601, *et seq.,* the Department of Commerce has prepared the following regulatory impact analysis (RIA) and initial regulatory flexibility analysis (IRFA) for this proposed rule.

1. Need for Regulatory Action

The reasons for and need for this action are summarized in this preamble. This rule is being proposed pursuant to E.O. 13984, ''Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities,'' and E.O. 14110, ''Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.'' As stated in E.O. 13984, ''Foreign actors use United States IaaS products for a variety of tasks in carrying out malicious cyber-enabled activities, which makes it extremely difficult for United States officials to track and obtain information through legal process before these foreign actors transition to replacement infrastructure and destroy evidence of their prior activities; foreign resellers of United States [IaaS] products make it easier for foreign actors to access these products and evade detection.'' Furthermore, E.O. 14011 states that ''irresponsible use could exacerbate societal harms such as fraud, discrimination, bias, and disinformation; displace and disempower workers; stifle competition; and pose risks to national security.'' To address these threats, E.O. 13984 requires the Secretary to propose regulations ''that require United States Infrastructure as a Service (IaaS) providers to verify the identity of a foreign person that obtains an Account.'' These regulations must also require U.S. IaaS providers to verify the identity of foreign customers, and the E.O. authorizes the Secretary to limit certain foreign actors' access to U.S. IaaS products. E.O. 14110 adds to these requirements by requiring the Secretary to propose regulations that require U.S. IaaS providers to ensure that foreign resellers of U.S. IaaS products verify the identity of any foreign person that obtains an IaaS Account for the foreign reseller. These requirements are necessary to protect the national security of the United States and the integrity of the ICTS supply chain.

2. Affected Entities

The proposed rulemaking would apply to all U.S. providers of U.S. IaaS products, including resellers.

3. Number of Affected Entities

The Department estimated both a lower and upper bound for the number of entities affected by the proposed rule. To derive the lower bound estimate, the Department first identified a core group of IaaS providers that operate in the United States. This lower bound estimate assumes that all United States IaaS products are sold directly to the customer and no domestic resellers supply these products. Based on this lower bound estimate, the Department estimates that approximately 25 providers in the United States would be potentially directly impacted by this rulemaking.

The upper bound estimate of potentially impacted entities is based on the estimated number of resellers who participate in the sale of U.S. IaaS products. According to the Census Bureau, in 2020 there were 1,812 firms that owned at least one establishment located within the United States and operating in North American Industry Classification System (NAICS) code 517121—Telecommunication Resellers in the United States.[1] While most of these entities would not likely be impacted by this proposed rule as they do not resell IaaS products or services, the Department uses this figure as the upper bound estimate for this impact statement because it is possible all of the Telecommunications Resellers could engage in IaaS product resale. The Department therefore estimates the number of entities potentially affected by this rulemaking would be between 25 and 1,837. Of those firms operating in the Telecommunications Resellers industry under NAICS 51721, 99 percent, or 1,791 firms, operate an enterprise size of 500 or fewer employees. This data underscores that the majority of listed entities in this sector can be classified as small businesses based on this specific definition.

4. Administrative Compliance Burden on U.S. Companies

The Department assessed the administrative compliance burden on U.S. companies by estimating the costs of: (1) learning about the proposed rule; (2) developing CIPs; (3) implementing CIPs; (4) updating CIPs; (5) completing annual certifications; (6) educating foreign resellers on CIP requirements; and (7) processing reporting from and on foreign resellers and foreign customers. Although the rulemaking would provide certain regulatory alternatives for industry, such as the option to adopt the CIP of another provider, and exemptions from the CIP requirement in certain circumstances, the below analysis assumes that each company would engage in the development, implementation, and updating of a CIP.

The Department also requests public comment on any of the assumptions and estimates in this analysis.

i. Learning About the Proposed Rule

The Department expects that businesses learning about the proposed rule and its requirements would largely be accomplished by attorneys and operations managers. The Department's estimate for the cost to businesses of learning about the rulemaking is further derived from estimates of the number of firms potentially impacted by the rulemaking, the share of potentially impacted firms likely to devote time and resources to learning about the rulemaking, the number of hours needed to read and learn about the rulemaking, and the wages of the employees tasked with learning about the rulemaking. Table 1 provides a detailed breakdown of the framework for estimating these costs.

[1] A firm is a business organization consisting of one or more domestic establishments in the same geographic area and industry that were specified under common ownership or control. See: *https://www.census.gov/programs-surveys/susb/about/glossary.html.*

Table 1: Framework for Estimating Costs Associated with Learning about the Proposed Rule

Line	Item	Low Estimate	High Estimate	Basis for estimate
1	Entities potentially impacted by the proposed rule	25	1,837	Low estimate is based on a supply chain analysis of a core group of companies directly affected by the proposed rule. High estimate is based on an analysis of industries that resell IaaS products.
2	Share of potentially impacted entities likely to devote time and resources to learning about the proposed rule	0.5	0.9	At the low end we estimate half of potentially impacted entities will devote time and resources towards learning about the proposed rule. This assumes a large number of potentially impacted entities already collect similar identifying information from their customers. At the high end we estimate nearly

				all potentially impacted entities will devote time and resources towards learning about the proposed rule.
3	Entities likely to devote time and resources to learning about the proposed rule	13	1,653	Line 1 * Line 2
4	Operations manager hours	2	2	This is an estimate of how long it is likely to take an operations manager to read and understand the proposed rule.
5	Operations manager hourly wage, doubled to account for benefits and overhead ($)	118	118	This is the Bureau of Labor Statistics (BLS) estimate for the mean hourly wage of an operations manager, doubled to reflect benefits and overhead.
6	Operations manager cost per entity ($)	236	236	Line 4 * Line 5
7	Lawyer hours	10	10	This is an estimate of how long it is likely to take a lawyer to read and understand the proposed rule.
8	Lawyer hourly wage, doubled to account for benefits and overhead ($)	157	157	This is the BLS estimate for the mean hourly wage of a lawyer, doubled to reflect benefits and overhead.
9	Lawyer cost per entity ($)	1,570	1,570	Line 7 * Line 8
10	Total initial cost per entity to learn about proposed rule ($)	1,806	1,806	Line 6 + Line 9
11	Total initial cost to learn about proposed rule ($)	22,575	2,985,860	Line 3 * Line 10
12	Annualized cost per entity over 10 years at 7% rate ($)	240	240	Line 10 is a one-time cost per firm to learn about the proposed rule. Line 12 annualizes that one-time cost over 10

ii. Developing a CIP

To develop CIPs, companies would likely be required to assess their offerings of IaaS products, analyze relevant cybersecurity risks associated with these products, evaluate procedures for customer identity verification, and develop risk mitigation strategies.

To estimate the financial impact to businesses of developing a CIP, the Department estimated the number of firms likely impacted by the proposed rule, the share of potentially impacted firms likely to devote time and resources to developing a CIP, the number of hours needed to develop a CIP, and the wages of the employees tasked with developing a CIP. A detailed breakdown of the framework for estimating these costs can be found in table 2.

				years at a 7% discount rate.
13	Annualized cost per entity over 10 years at 3% rate ($)	206	206	Line 10 is a one-time cost per firm to learn about the proposed rule. Line 13 annualizes that one-time cost over 10 years at a 3% discount rate.
14	Total annualized costs at 7% discount rate ($)	3,004	397,308	Line 3 * Line 12
15	Total annualized costs at 3% discount rate ($)	2,569	339,839	Line 3 * Line 13

Table 2: Framework for Estimating Costs Associated with Developing a CIP

Line	Item	Low Estimate	High Estimate	Basis for estimate
1	Entities potentially impacted by the proposed rule	25	1,837	Low estimate is based on a supply chain analysis of a core group of companies directly affected by the proposed rule. High estimate is based on an analysis of

				industries that resell IaaS products.
2	Share of potentially impacted entities likely to devote time and resources to developing a CIP	0.8	1	The Department estimate that some entities already have performed the work needed to establish a CIP and thus will not need to devote time and resources to developing one. The high-end estimate assumes all providers will have to change their existing procedures to come into compliance with this proposed rule.
3	Entities likely to devote time and resources to developing a CIP	20	1,837	Line 1 * Line 2
4	Operations manager hours	80	80	This is an estimate of how long it is likely to take an operations manager to develop a CIP.
5	Operations manager hourly wage, doubled to account for benefits and overhead ($)	118	118	This is the BLS estimate for the mean hourly wage of an operations manager, doubled to reflect benefits and overhead.
6	Operations manager cost per entity ($)	9,440	9,440	Line 4 * Line 5
7	Total initial cost to develop a CIP ($)	188,800	17,341,280	Line 3 * Line 6
8	Annualized cost per entity over 10 years at 7% rate ($)	1,256	1,256	Line 6 is a one-time cost per firm to develop a CIP. Line 8 annualizes that one-time cost over 10 years at a 7% discount rate.

iii. Implementing the CIP

Implementation of a CIP would likely entail: collecting and verifying identifying information of customers, maintaining a secure recordkeeping system, performing due-diligence checks using government lists of known malicious cyber actors, and providing annual reports to the Department. The proposed rule would also require entities to monitor aspects of compliance with their foreign customers and resellers. The costs estimated for implementing a CIP would be incurred annually. To estimate the financial impact to businesses of implementing a CIP, the Department estimated the number of firms potentially impacted by the proposed rule, the share of potentially impacted firms likely to implement a CIP, and the wages of the employees performing these tasks. A detailed breakdown of the framework for estimating these costs can be found in table 3.

9	Annualized cost per entity over 10 years at 3% rate ($)	1,074	1,074	Line 6 is a one-time cost per firm to develop a CIP. Line 9 annualizes that one-time cost over 10 years at a 3% discount rate.
10	Total annualized costs at 7% discount rate ($)	25,122	2,307,484	Line 3 * Line 8
11	Total annualized costs at 3% discount rate ($)	21,488	1,973,716	Line 3 * Line 9

Table 3: Framework for Estimating Costs Associated with Implementing a CIP

Line	Item	Low Estimate	High Estimate	Basis for estimate
1	Entities potentially impacted by the proposed rule	25	1,837	Low estimate is based on a supply chain analysis of a core group of companies directly affected by the proposed rule. High estimate is based on

				an analysis of industries that resell IaaS products.
2	Share of potentially impacted entities likely to devote time and resources to implementing a CIP	0.8	1	We expect all entities that develop a CIP will implement the CIP. Thus, these estimates are identical to those in table 2.
3	Entities likely to devote time and resources to implementing a CIP	20	1,837	Line 1 * Line 2
4	Number of new Accounts subject to the proposed rule per firm per year	100	1,000	This is an estimate of the number of transactions for each provider likely to be subject to CIP requirements in a given year.
5	Operations manager hours to perform analysis and due diligence per new account	0.3	0.3	This is an estimate of the number of hours we expect would be needed to collect customer identification information and verify that information.
6	Total Operations manager hours to perform analysis and due diligence per new account	33	330	Line 4 * Line 5
7	Operations manager hourly wage, doubled to account for benefits and overhead ($)	118	118	This is the BLS estimate for the mean hourly wage of an operations manager, doubled to reflect benefits and overhead.
8	Operations manager cost per transaction ($)	39	39	Line 5 * Line 7
9	Operations manager annual cost per entity ($)	3,894	38,940	Line 4 * Line 8
10	Total annual cost ($)	77,880	71,532,780	Line 3 * Line 9

iv. Updating the CIP

The proposed rule would require that affected entities regularly, at least annually, update their CIPs to account for new technologies, cybersecurity vulnerabilities, and changes to their business. This would likely entail reviewing the threat landscape from the previous year and identifying system vulnerabilities. Table 4 details the estimated financial impact to businesses of annually updating a CIP.

Table 4: Framework for Estimating Costs Associated with Updating the CIP

Line	Item	Low Estimate	High Estimate	Basis for estimate
1	Entities potentially impacted by the proposed rule	25	1,837	Low estimate is based on a supply chain analysis of a core group of companies directly affected by the proposed rule. High estimate is based on an analysis of industries that resell IaaS products.
2	Share of potentially impacted entities likely to devote time and resources to updating a CIP	0.8	1	We expect all entities that develop a CIP will conduct an annual update. Thus, these estimates are identical to those in tables 2 and 3.
3	Entities likely to devote time and resources to updating a CIP	20	1,837	Line 1 * Line 2
4	Number of CIP updates necessary annually	1	3	Low estimate is based on the assumption that businesses are only updating their CIPs once annually. High estimate is based on 2 off-cycle major changes in the business and threat landscape requiring additional updates.
5	Operations manager hours to review and assess service	20	80	We estimate 0.5 to 2 weeks, depending on the complexity of business

	offerings, threat landscape, and failure to verify customer identities			changes, magnitude of threats faced, and depth of customer base.
6	Operations manager hourly wage, doubled to account for benefits and overhead ($)	118	118	This is the BLS estimate for the mean hourly wage of an operations manager, doubled to reflect benefits and overhead.
7	Operations manager cost per update ($)	2,360	9,440	Line 5 * Line 6
8	Lawyer hours to review CIP updates	16	24	We estimate approximately 2-3 days to review updated CIPs.
9	Lawyer hourly wage, doubled to account for benefits and overhead ($)	157	157	This is the BLS estimate for the mean hourly wage of a lawyer, doubled to reflect benefits and overhead.
10	Lawyer cost per update ($)	2,512	3,768	Line 8 * Line 9
11	Total cost per update ($)	4,872	13,208	Line 7 + Line 10
12	Annual cost per entity($)	4,872	39,624	Line 11 * Line 4
13	Total annual cost ($)	97,440	72,789,288	Line 12 * Line 3

v. Annual Certifications

The proposed rule would require IaaS providers to annually certify to the Department that they have updated their CIP, that their CIP complies with the rulemaking, and that they have recorded the resolution of each situation in which the IaaS provider was unable to verify the identity of a customer since its last certification.

The estimated costs of submitting annual certifications would occur annually. This estimate for costs is derived from estimates of the number of firms impacted by the proposed rule, the share of potentially impacted firms likely to submit the annual certifications, and the wages of the employees performing these tasks. A detailed breakdown of the framework for estimating these costs can be found in table 5.

Table 5: Framework for Estimating Costs Associated with Annual Certifications

Line	Item	Low Estimate	High Estimate	Basis for estimate
1	Entities potentially impacted by the proposed rule	25	1,837	Low estimate is based on a supply chain analysis of a core group of companies directly affected by the proposed rule. High estimate is based on an analysis of industries that resell IaaS products.
2	Share of potentially impacted entities likely to devote time and resources to submitting annual certifications.	0.8	1	We expect all entities that develop a CIP will submit an Annual Certification. Thus, these estimates are identical to those in tables 2 and 3.
3	Entities likely to devote time and resources to submitting annual certifications.	20	1,837	Line 1 * Line 2
4	Operations manager hours to review prior year compliance, CIP updates, and submit certification.	8	24	This is an estimate of the time needed to evaluate the provider's customer base, account offerings, and current vulnerabilities to prepare the annual certification.
5	Operations manager hourly wage, doubled to account for benefits and overhead ($)	118	118	This is the BLS estimate for the mean hourly wage of an operations manager, doubled to reflect benefits and overhead.
6	Operations manager cost per entity ($)	944	2,832	Line 4 * Line 5

7	Total Annual Operations manager cost ($)	18,880	5,202,384	Line 3 * Line 6
8	Lawyer hours to review annual recertifications	5	5	This is an estimate of the time needed for a lawyer to review a provider's annual certification prior to submission to the Department
9	Lawyer hourly wage, doubled to account for benefits and overhead ($)	157	157	This is the BLS estimate for the mean hourly wage of a lawyer, doubled to reflect benefits and overhead.
10	Lawyer cost per annual certifications ($)	785	785	Line 8 * Line 9
11	Total annual lawyer cost ($)	15,700	1,442,045	Line 3 * Line 10
12	Total annual cost ($)	34,580	6,644,429	Line 7 + Line 11

vi. Foreign Reseller Requirements

The burden of learning about the proposed rule, and developing, maintaining, and recertifying CIPs for foreign resellers would fall upon foreign entities (the foreign resellers themselves). However, the Department recognizes that U.S. IaaS providers would be part of educating foreign resellers on regulatory requirements. U.S. IaaS providers would also need to collect and submit CIPs from foreign resellers. The Department anticipates that foreign resellers of U.S. IaaS providers would comply with the regulatory requirements, so does not anticipate there to be impact beyond the regulatory costs of compliance (which will fall to foreign entities), and the burden on U.S. providers to educate foreign resellers and process foreign reseller CIPs.

The Department recognizes that individual costs to industry would vary according to the number of foreign resellers connected to a U.S. IaaS provider. However, the Department is unable to estimate the potential number of foreign resellers of U.S. IaaS products, as this information is business proprietary information held by the U.S. IaaS providers. Following the implementation of CIP reporting requirements to the Department, the Department may be able to estimate a lower bound and upper bound on potential cost per CIP certification. However, at this time, due to the described limitations, the cost estimates have been made on a programmatic basis as opposed to a per CIP certification basis.

vii. Educating Foreign Resellers on U.S. CIP Requirements

U.S. IaaS providers would be required to ensure their foreign resellers comply with this proposed rule and to ensure they receive CIPs from their foreign resellers. This could involve notifying their foreign resellers of this proposed rule's requirements, advising foreign resellers on CIP solutions or processes, and generally educating foreign resellers about this rulemaking.

This estimate for costs is derived from estimates of the number of U.S. firms impacted by the proposed rule, the share of potentially impacted firms to educate their foreign resellers, and the wages of the employees performing these tasks. A detailed breakdown of the framework for estimating these costs can be found in table 6.

Table 6: Framework for Estimating Costs for U.S. IaaS Providers to Educate Foreign Resellers on U.S. CIP Requirements

Line	Item	Low Estimate	High Estimate	Basis for estimate
1	Entities potentially impacted by the proposed rule	25	1,837	Low estimate is based on a supply chain analysis of a core group of companies directly affected by the proposed rule. High estimate is based on an analysis of industries that resell IaaS products.
2	Share of potentially impacted entities likely to devote time and resources to educating their foreign resellers about the proposed rule	0.25	0.75	The Department estimates that roughly half of U.S. IaaS providers have at least one foreign reseller and will consequently devote

				time to educating the reseller on the provisions of this proposed rule. Given that most foreign reseller arrangements are not public information, the Department seeks comment on this estimate.
3	Entities likely to devote time and resources to educating their foreign resellers about the proposed rule	6	1,378	Line 1 * Line 2
4	Operations manager hours to educate their foreign resellers about the proposed rule	120	120	This is an estimate of the number of hours we expect would be needed for an operations manager to educate their foreign resellers about the proposed rule and aid them in developing and running a program. We estimate approximately 3 weeks, based on the 2 weeks estimated for an operations manager to develop a CIP (table 2), plus an additional 1 week.
5	Operations manager hourly wage, doubled to account for benefits and overhead ($)	118	118	This is the BLS estimate for the mean hourly wage of an operations manager, doubled to reflect benefits and overhead.
6	Operations manager cost per entity ($)	14,160	14,160	Line 4 * Line 5
7	Lawyer hours to consult with operations managers and foreign resellers about foreign reseller CIP requirements	10	10	We estimate approximately 10 hours of work spread out over the course of a year.
8	Lawyer hourly wage, doubled to account for benefits and overhead ($)	157	157	This is the BLS estimate for the mean hourly wage of a lawyer, doubled to reflect benefits and overhead.
9	Lawyer cost per entity ($)	1,570	1,570	Line 7 * Line 8

viii. Processing Reporting From Foreign Resellers and on AI Training Runs

The costs to U.S. IaaS providers associated with processing reporting from foreign resellers include costs of collecting and submitting to the Department upon request the CIPs from any foreign resellers, as well as any associated miscellaneous administrative costs. Processing reporting also would include U.S. IaaS providers' activities to report on any of their foreign customers using their U.S. IaaS products in a covered transaction for large AI model training. These would be annual costs.

This estimate for costs is derived from estimates of the number of U.S. firms impacted by the proposed rule, the share of potentially impacted firms that need to process foreign reseller CIPs and reports on foreign customers using their U.S. IaaS products in a covered transaction for large AI model training, and the wages of the employees performing these tasks. A detailed breakdown of the framework for estimating these costs can be found in table 7.

10	Total initial costs per entity to educate foreign resellers ($)	15,730	15,730	Line 6 + Line 9
11	Total initial costs to educate foreign resellers ($)	98,313	21,672,008	Line 3 * Line 10
12	Annualized cost per entity over 10 years at 7% rate ($)	2,093	2,093	Line 10 is a one-time cost per firm to learn about the proposed rule. Line 12 annualizes that one-time cost over 10 years at a 7% discount rate.
13	Annualized cost per entity over 10 years at 3% rate ($)	1,790	1,790	Line 10 is a one-time cost per firm to learn about the proposed rule. Line 13 annualizes that one-time cost over 10 years at a 3% discount rate.
14	Total annualized costs at 7% discount rate ($)	13,082	2,883,744	Line 3 * Line 12
15	Total annualized costs at 3% discount rate ($)	11,190	2,466,622	Line 3 * Line 13

Table 7: Framework for Estimating Costs for U.S. IaaS Providers to Process Reporting from Foreign Resellers and on AI Training Runs

Line	Item	Low Estimate	High Estimate	Basis for estimate
1	Entities potentially impacted by the proposed rule	25	1,837	Low estimate is based on a supply chain analysis of a core group of companies directly affected by the proposed rule. High estimate is based on an analysis of industries that resell IaaS products.
2	Share of potentially impacted entities likely to devote time and resources to processing reporting from and on foreign resellers and foreign customers	0.25	0.75	The Department estimates that roughly half of U.S. IaaS providers have at least one foreign reseller and will consequently dedicate time to processing the reporting from the reseller(s) pursuant to this proposed rule. As such, this calculation is identical to the one in table 6, and the Department similarly seeks comment on this estimate.
3	Entities likely to devote time and resources to processing reporting from and on foreign resellers and foreign customers	6	1,378	Line 1 * Line 2
4	Operations manager hours to process reporting from and on foreign resellers and foreign customers	8	40	This is an estimate of the number of hours we expect would be needed for an operations manager to intake, review, collate, and submit to the Department the reporting from foreign resellers. We estimate approximately 1 day to 1 week of work spread out over the course of a year, depending on the number of foreign resellers and scope of their business.
5	Operations manager hourly wage, doubled to	118	118	This is the BLS estimate for the mean hourly wage of an operations manager, doubled

5. Potential Economic Impact of the Proposed Rule

Using the methodology described above, the Department has broken out the estimated compliance costs—summarized in tables 8 and 9—associated with the proposed rule's implementation. The cumulative costs are estimated to be between $270,672 and $171.7 million.

	account for benefits and overhead ($)			to reflect benefits and overhead.
6	Operations manager cost per entity ($)	944	4720	Line 4 * Line 5
7	Total Annual Operations manager cost ($)	5,900	6,502,980	Line 3 * Line 6
8	Lawyer hours to advise on reporting from and on foreign resellers and foreign customers	20	40	We estimate approximately 0.5-1 week of work spread out over the course of a year to support operations managers in the review and submission to the Department of foreign reseller reporting.
9	Lawyer hourly wage, doubled to account for benefits and overhead ($)	157	157	This is the BLS estimate for the mean hourly wage of a lawyer, doubled to reflect benefits and overhead.
10	Lawyer cost per entity ($)	3,140	6,280	Line 8 * Line 9
11	Total Annual Lawyer cost ($)	19,625	8,652,270	Line 3 * Line 10
12	Total annual cost ($)	25,525	15,155,250	Line 7 + Line 11

Table 8: Estimates for the Cost of the IaaS Proposed Rule (Annualized at 7%)

Aggregate Costs to Businesses (Annualized at 7%)	Low Estimate	High Estimate
1. Learning about the proposed rule (annualized at 7%)	$3,004	$397,308
2. Developing a CIP (annualized at 7%)	$25,122	$2,307,484
3. Implementing the CIP	$77,880	$71,532,780
4. Updating the CIP	$97,440	$72,789,288
5. Annual Certifications	$34,580	$6,644,429
6. Education on U.S. CIP Requirements (annualized at 7%)	$13,082	$2,883,744
7. Processing Reports on and from Foreign Entities	$25,525	$15,155,250
Total (annualized at 7%)	$276,633	$171,710,283

Table 9: Estimates for the Cost of the IaaS Proposed Rule (Annualized at 3%)

Aggregate Costs to Businesses (Annualized at 3%)	Low Estimate	High Estimate
1. Learning about the proposed rule (annualized at 3%)	$2,569	$339,839
2. Developing a CIP (annualized at 3%)	$21,488	$1,973,716
3. Implementing the CIP	$77,880	$71,532,780
4. Updating the CIP	$97,440	$72,789,288
5. Annual Certifications	$34,580	$6,644,429
6. Education on U.S. CIP Requirements (annualized at 3%)	$11,190	$2,466,622
7. Processing Reports on and from Foreign Entities	$25,525	$15,155,250
Total (annualized at 3%)	$270,672	$170,901,923

6. Benefits of the Proposed Rule

The ICTS industry, which includes IaaS products, has become integral to the daily operations and functionality of U.S. critical infrastructure, to U.S. Government operations, and to the U.S. economy as a whole. As such, exploitation of vulnerabilities within the ICTS supply chain can have a drastic effect on the U.S. national security. As noted in E.O. 13984, ''foreign malicious cyber actors aim to harm the United States economy through the theft of intellectual property and sensitive data and to threaten national security by targeting United States critical infrastructure for malicious cyber-enabled activities.''

U.S. entities providing IaaS products, such as network management or data storage, can create multiple opportunities for foreign adversaries to exploit potential vulnerabilities in the ICTS ecosystem. These potential vulnerabilities are often categorized under the general concepts of threats to privacy, data integrity, and denial of service.

As E.O. 13984 highlights, foreign actors can exploit IaaS product vulnerabilities to steal critical intellectual property, health data, government information, or financial user information, potentially without detection. Once detected, the existence of such vulnerabilities may be extremely costly or impossible to remedy.

Malicious foreign actors can also exploit U.S. networks and systems to facilitate data breaches, potentially modifying critical files or data streams, or otherwise impacting the availability of data across U.S. networks. Such capabilities could be exercised in areas as diverse as financial market communications, satellite control systems, or other sensitive sectors.

Further, a foreign adversary could target vulnerable IaaS products to implement denial of service attacks, potentially causing widespread disruptions to critical industries. Without effective attribution, it is difficult for authorities to take mitigating actions to trace and prevent these types of attacks.

These risks, if exploited, could carry significant economic and social costs to both the U.S. Government and consumers. Sophisticated cyber-attacks are often obfuscated, making it difficult to establish the exact number of attacks that have leveraged IaaS product vulnerabilities against the U.S. ICTS supply chain. Such attacks, however, are increasing in frequency, exacting heavy tolls on U.S. consumers and businesses. Not only can attacks impact both sales and productivity, but they can also enact direct costs on businesses that must expend significant resources to remedy vulnerabilities or even pay ransom to retrieve data lost to attackers. While the Department is unable to calculate with certainty the number of attacks targeting the IaaS industry, the potential costs from these attacks are undoubtedly high. Additionally, if the use of IaaS products is expected to increase in the future, so too would the possibility of attacks. While the Department lacks the data necessary to determine precisely the monetary benefits of this proposed rule to compare with its estimated costs, significant portions of the U.S. economy are dependent on resilient ICTS and IaaS supply chains to function, and any disruption to these supply chains will cause significant economic harm to downstream industries.

7. Regulatory Alternatives

The Department considered several alternatives to this regulation to reduce the costs. These are explained in detail in subpart C, Regulatory Flexibility Analysis, of this section, below.

A. Regulatory Flexibility Act

In compliance with section 603 of the Regulatory Flexibility Act (RFA), 5 U.S.C. 601–612, the Department has prepared an initial regulatory flexibility analysis (IRFA) for this proposed rule. The IRFA describes the economic impacts the proposed action may have on small entities. The Department seeks comments on all aspects of the IRFA, including the categories and numbers of small entities that may be directly impacted by this proposed rule.

(1) *A description of the reasons why action by the agency is being considered.* The description of the reasons why the proposed rule is being considered is contained earlier in the preamble and is not repeated here.

(2) *A succinct statement of the objectives of, and legal basis for, the proposed rule.* The Department is proposing this rule to comply with Executive Order 13984, ''Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities'' (86 FR 6387), and E.O. 14110, ''Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence'' (88 FR 75191). E.O. 13984 directs the Secretary to propose regulations requiring U.S. IaaS providers to collect customer identifying information from prospective customers and to verify the identity of all foreign customers. This E.O. further requires the Secretary to propose regulations authorizing the

Secretary to utilize one of two special measures to limit or prohibit specific IaaS Accounts should the Secretary, in consultation with various heads of other Executive agencies, determine that reasonable grounds exist to conclude the IaaS Account is being used to conduct malicious, cyber-enabled activity. E.O. 14110 also requires the Secretary to propose regulations that require U.S. IaaS providers report to the Department when they transact with a foreign reseller to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity.

(3) *A description of, and where feasible, an estimate of the number of small entities to which the proposed rule will apply.* The proposed rule would apply to all providers of U.S. IaaS products, including resellers. The Department acknowledges that actions taken pursuant to this proposed rule may affect small entities or groups that are not easily categorized at present. The Department assesses, based on publicly available information, that the IaaS market is dominated by four large providers; however, it is difficult to ascertain how many small entities, are present in this market. For resellers, Survey of U.S. Business Data suggests that approximately 99 percent of the roughly 1,800 enterprises categorized as ''Telecommunications Resellers'' under NAICS code 517911 have fewer than 500 employees, indicating that the vast number of those resellers would be small businesses under the Small Business Administration (SBA) threshold for this NAICS code (*https://www.sba.gov/document/support-table-size-standards*). However, the Department lacks data on the number of these Telecommunications Resellers that offer IaaS products.

(4) *A description of the projected reporting, recordkeeping and other compliance requirements of the proposed rule, including an estimate of the classes of small entities that will be subject to the requirement and the type of professional skills necessary for preparation of the report or record.* The proposed rule would impose on all U.S. IaaS providers of U.S. IaaS products a new requirement to identity and verify the identity of all foreign customers. It would require providers to ensure that foreign resellers of their U.S. IaaS products verify the identity of foreign users. It would require all U.S. IaaS providers of U.S. IaaS products to report to the Department information on instances of training runs by foreign persons for large AI model with potential capabilities that could be used in malicious cyber-enabled activity. Finally, it would require providers to submit annual certifications attesting to the Department that they have reviewed their CIPs and adjusted them to account for changes to the threat landscape since their prior certification. The Department believes this requirement would create the following recordkeeping obligations:

(i) The proposed rule would require that the customer identification and verification requirement be satisfied by obtaining identification information from each customer. The provider would then be required to verify customer identities through documentary or non-documentary methods and to maintain in its records for two years a description of (i) any document relied on for verification, (ii) any such non-documentary methods and results of such measures undertaken, and (iii) the resolution of any substantive discrepancies discovered in verifying the identification information. The Department estimates that the identification, verification, and recordkeeping requirements in the proposed rule would require an IaaS provider employee twenty (20) minutes, on average, to fulfill.

(ii) Annual Certifications. The proposed rule would require that U.S. IaaS providers of U.S. IaaS products provide to the Department annual certifications that indicate that the provider has updated their customer identification program to account for technological advances and the evolving threat landscape. The Department estimates it would require eight (8) to twenty-four (24) hours to review prior year compliance, complete CIP updates, and submit certification.

(iii) The proposed rule would require providers to submit a 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. The Department estimates that an IaaS provider making a report on such a transaction could take on average twenty (20) minutes, depending on the complexity of the instance.

(5) *An identification, to the extent practicable, of all relevant Federal rules that may duplicate, overlap or conflict with the proposed rule.* This rulemaking does not duplicate or conflict with any Federal rules.

(6) *A description of any significant alternatives to the proposed rule that accomplish the stated objectives of Executive Order 13984 and Executive Order 14110 and applicable statutes and that would minimize any significant economic impact of the proposed rule on small entities.*

- *No-action alternative:* Not implementing a rule under these Executive orders (E.O.s) is not a viable alternative because both E.O.s expressly direct that the Secretary ''shall propose for notice and comment regulations'' given the related national security concerns associated with malicious cyber-enabled activities through the use of U.S. IaaS products.
- *Alternative that would categorically exclude small entities or groups of small entities:* This alternative would not achieve the national security objectives of these E.O.s. Due to the nature of ICTS networks, allowing even small entities or groups of small entities unregulated access to IaaS products or services can allow malicious actors to perpetrate attacks on the entire network, posing an undue risk to U.S. critical infrastructure and the U.S. economy as a whole.
- *Preferred alternative:* The proposed rule is the preferred alternative. It would achieve the objectives of the E.O.s by requiring IaaS providers to verify customer identities and facilitating the implementation of special measures that would allow the Secretary to apply a case-by-case, fact-specific process to identify, assess, and address any and all IaaS Accounts that pose an undue risk to the U.S. national security. The proposed rule also offers an exemption program that would offer providers an alternative to the CIP requirements to reduce their compliance burdens, as providers can decide whether it is less burdensome to implement a CIP or to apply for an exemption.

B. Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*) (PRA) provides that an agency generally cannot conduct or sponsor a collection of information, and no person is required to respond to nor be subject to a penalty for failure to comply with a collection of information subject to the requirements of the PRA, unless that collection has obtained Office of Management and Budget (OMB) approval and displays a currently valid OMB Control Number.

This proposed rule contains new collection-of-information requirements subject to review and approval by OMB under the PRA. Specifically, this proposed rule would require U.S. IaaS providers of U.S. IaaS products to develop a written CIP, which dictates how the provider would collect identifying information about its customers, how the provider would verify the identity of its foreign customers, store and maintain

identifying information, and notify its customers about the disclosure of identifying information. Additionally, the proposed rule would require providers to report to the Department information on instances of training runs by foreign persons for large AI models with potential capabilities that could be used in malicious cyber-enabled activity. The Department requests comment on what additional information, if any, the Department should require providers report. Moreover, the proposed rule would require that U.S. IaaS providers of U.S. IaaS products submit to the Department an initial certification, and subsequent annual certifications, detailing certain aspects of their CIPs and stating that they have reviewed their CIP and adjusted it to account for changes to the threat landscape since their prior certification. These certifications would also include an attestation that the current CIP complies with the provisions of the proposed rule. The attestations would require the provider to indicate the frequency with which it was unable to verify the identity of a foreign customer in the prior calendar year and the number of times the provider refused to open an Account.

Alternatively, under the proposed rule, U.S. IaaS providers of U.S. IaaS products may seek an exemption from the CIP requirement by providing a written submission to the Secretary. Should the Secretary grant an exemption on the basis of a finding that the provider complies with security best practices to deter abuse of IaaS products, including that the provider has established an Abuse of IaaS Products Deterrence Program, the provider must thereafter submit annual notifications to the Department so that the Department could be assured that it continues to maintain security best practices to deter the abuse of U.S. IaaS products.

Public reporting burden for the reporting and recordkeeping requirements are estimated to average 245,229 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 proposed 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.

The total estimated cost 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.

The Department requests comments on the information collection and recordkeeping requirements associated with this proposed rule. These comments will help the Department:

(i) evaluate whether the information collection is necessary for the proper performance of our agency's functions, including whether the information will have practical utility;

(ii) evaluate the accuracy of our estimate of the burden of the information collection, including the validity of the methodology and assumptions used;

(iii) enhance the quality, utility, and clarity of the information to be collected; and

(iv) minimize the burden of the information collection on those who are to respond (such as through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, *e.g.,* permitting electronic submission of responses).

C. Unfunded Mandates Reform Act of 1995

This proposed rule would not produce a Federal mandate (under the regulatory provisions of title II of the Unfunded Mandates Reform Act of 1995) for State, local, and tribal governments or the private sector.

D. Executive Order 13132 (Federalism)

This proposed rule does not contain policies having federalism implications requiring preparations of a Federalism Summary Impact Statement.

E. Executive Order 12630 (Governmental Actions and Interference With Constitutionally Protected Property Rights)

This proposed rule does not contain policies that have takings implications.

F. Executive Order 13175 (Consultation and Coordination With Indian Tribes)

The Department has analyzed this proposed rule under Executive Order 13175 and has determined that the action would not have a substantial direct effect on one or more Indian tribes, would not impose substantial direct compliance costs on Indian tribal governments, and would not preempt tribal law.

G. National Environmental Policy Act

The Department has reviewed this rulemaking action for the purposes of the National Environmental Policy Act (42 U.S.C. 4321 *et seq.*). It has determined that this proposed rule would not have a significant impact on the quality of the human environment.

List of Subjects in 15 CFR Part 7

Administrative practice and procedure, Business and industry, Communications, Computer technology, Critical infrastructure, Executive orders, Foreign persons, Investigations, National security, Penalties, Technology, Telecommunications.

For the reasons set out in the preamble, 15 CFR part 7 is proposed to be amended as follows:

PART 7—SECURING THE INFORMATION AND COMMUNICATIONS TECHNOLOGY AND SERVICES SUPPLY CHAIN

■ 1. The authority citation for part 7 is revised to read as follows:

Authority: 50 U.S.C. 1701, *et seq.;* 50 U.S.C. 1601, *et seq.;* E.O. 13873, 84 FR 22689, 3 CFR, 2019 Comp., p. 317; E.O. 13984, 86 FR 6837, 3 CFR, 2021 Comp., p. 403.

■ 2. Add subpart D, consisting of §§ 7.300 through 7.310, to read as follows:

Subpart D—Infrastructure as a Service Providers' Responsibility To Verify the Identity of Their Customers, Special Measures, and the Use of Their Products for Large AI Model Training

Sec.

§ 7.300 Purpose and scope.

Foreign actors may use United States Infrastructure as a Service (IaaS) products for a variety of malicious cyber-enabled activities. In light of these threats, it is the purpose of this subpart to:

(a) Require U.S. IaaS providers of U.S. IaaS products to implement programs to maintain certain records related to IaaS Accounts in which foreign persons have an interest and verify the identity of such persons, and to require their foreign resellers to do the same, in order to facilitate law enforcement requests for such records and otherwise implement the provisions of Executive Order 13984 and Executive Order 14110;

(b) Prevent foreign persons from using U.S. IaaS products to conduct malicious cyber-enabled activities; and

(c) Safeguard the national security of the United States.

§ 7.301 Definitions and application.

For the purposes of this subpart:

Artificial intelligence or *AI* has the meaning set forth in 15 U.S.C. 9401(3).

AI model means a component of an information system that implements AI technology and uses computational, statistical, or machine-learning techniques to produce outputs from a given set of inputs.

AI system means any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI.

Availability means ensuring timely and reliable access to and use of information and information systems by an authorized person or system, including resources provided as part of a product or service.

Beneficial owner means an individual who either:

(1) Exercises substantial control over a customer; or

(2) Owns or controls at least 25 percent of the ownership interests of a customer.

Confidentiality means preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Customer means any individual or entity who contracts with an IaaS provider to create or maintain an IaaS Account with an IaaS provider.

Customer Identification Program or *CIP* means a program created by a United States IaaS provider of U.S. IaaS products that dictates how the provider will collect identifying information about its customers, how the provider will verify the identity of its foreign customers, store and maintain identifying information, and notify its customers about the disclosure of identifying information.

Department means the United States Department of Commerce.

Disassociability means enabling the processing of data or events without association to individuals or devices beyond the operational requirements of the system.

Dual-use foundation model means:

(1) An AI model that is trained on broad data; generally uses self-supervision; contains at least tens of billions of parameters; is applicable across a wide range of contexts; and that exhibits, or could be easily modified to exhibit, high levels of performance at tasks that pose a serious risk to security, national economic security, national public health or safety, or any combination of those matters, such as by:

(i) Substantially lowering the barrier of entry for non-experts to design, synthesize, acquire, or use chemical, biological, radiological, or nuclear (CBRN) weapons;

(ii) Enabling powerful offensive cyber operations through automated vulnerability discovery and exploitation against a wide range of potential targets of cyber attacks; or

(iii) Permitting the evasion of human control or oversight through means of deception or obfuscation.

(2) Models meet this definition even if they are provided to end users with technical safeguards that attempt to prevent users from taking advantage of the relevant unsafe capabilities.

Entity means a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization.

Floating-point operation means any mathematical operation or assignment involving floating-point numbers, which are a subset of the real numbers typically represented on computers by an integer of fixed precision scaled by an integer exponent of a fixed base.

Foreign beneficial owner means a beneficial owner that is not a United States person.

Foreign customer means a customer that is not a United States person.

Foreign jurisdiction means any country, subnational territory, or region, other than those subject to the civil or military jurisdiction of the United States, in which any person or group of persons exercises sovereign de facto or de jure authority, including any such country, subnational territory, or region in which a person or group of persons is assuming to exercise governmental authority whether such a person or group of persons has or has not been recognized by the United States.

Foreign person means a person that is not a United States person.

Foreign reseller or *foreign reseller of U.S. Infrastructure as a Service products* mean a foreign person who has established an Infrastructure as a Service Account to provide Infrastructure as a Service products subsequently, in whole or in part, to a third party.

Generative AI means the class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content. This can include images, videos, audio, text, and other digital content.

Individual means any natural person.

Infrastructure as a Service Account or *Account* means a formal business relationship established to provide IaaS products to a person in which details of such transactions are recorded.

Infrastructure as a Service product or *IaaS product* means a product or service offered to a consumer, including complimentary or ''trial'' offerings, that provides processing, storage, networks, or other fundamental computing resources, and with which the consumer is able to deploy and run software that is not predefined, including operating systems and applications. The consumer typically does not manage or control most of the underlying hardware but has control over the operating systems, storage, and any deployed applications. The term is inclusive of ''managed'' products or services, in which the provider is responsible for some aspects of system configuration or maintenance, and ''unmanaged'' products or services, in which the provider is only responsible for ensuring that the product is available to the consumer. The term is also inclusive of ''virtualized'' products and services, in which the computing resources of a physical machine are split between virtualized computers accessible over the internet (*e.g.,* ''virtual private servers''), and ''dedicated'' products or services in which the total computing resources of a physical machine are provided to a single person (*e.g.,* ''bare-metal servers'').

Integer operation means any mathematical operation or assignment involving only integers, or whole numbers expressed without a decimal point.

Integrity means guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.

Knowledge has the meaning set out in 15 CFR 772.1.

Large AI model with potential capabilities that could be used in malicious cyber-enabled activity means 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, including but not limited to social engineering attacks, vulnerability discovery, denial-of-service attacks, data poisoning, target selection and prioritization, disinformation or misinformation generation and/or propagation, and remote command-and-control of cyber operations. A model shall be considered to be a large AI model with potential capabilities that could be used in malicious cyber-enabled activity under this definition if it meets the technical conditions described in interpretive rules issued by the Department and published in the **Federal Register**.

Machine learning means a set of techniques that can be used to train AI algorithms on data to improve performance at a task or tasks.

Malicious cyber-enabled activities means activities, other than those authorized by or in accordance with U.S. law, that seek to compromise or impair the confidentiality, integrity, or availability of computer, information, or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.

Manageability means providing the capability for granular administration of data, including alteration, deletion, and selective disclosure.

Model weight means a numerical parameter within an AI model that helps determine the model's outputs in response to inputs.

Predictability means enabling reliable assumptions by individuals, owners, and operators about data and their processing by a system, product, or service.

Person means an individual or entity.

Privacy-preserving data sharing and analytics means the use of privacy-enhancing technologies to achieve disassociability, predictability, manageability, and confidentiality when performing analytics on data.

Red Flag means a pattern, practice, or specific activity that indicates the possible existence of malicious cyber-enabled activities.

Reseller means a person that maintains a Reseller Account.

Reseller Account means an Infrastructure as a Service Account established to provide IaaS products to a person who will then offer those products subsequently, in whole or in part, to a third party.

Risk-based means based on an appropriate assessment of the relevant risks, including those presented by the various types of service offerings maintained by the provider, the methods used to open an Account, the varying types of identifying information available to the provider, and the provider's customer base.

Secretary means the Secretary of Commerce or the Secretary's designee.

Threat landscape means the broad environment of geopolitical, economic, and technological factors that must be evaluated when developing risk-based procedures that enable the provider to form a reasonable belief of the true identity of each account owner and beneficial owner to deter facilitating significant Malicious cyber-enabled activities.

Training or *training run* refers to any process by which an AI model learns from data using computing power.

Transaction means any transfer of value including any of the following, whether proposed or completed: an exchange of value for a good or service; a merger, acquisition, or takeover; an investment; and any other transfer, agreement, or arrangement, the structure of which is designed or intended to evade or circumvent the application of § 7.307.

United States Infrastructure as a Service product or *U.S. IaaS product* means any Infrastructure as a Service product owned by any United States person or operated within the territory of the United States.

United States Infrastructure as a Service provider or *U.S. IaaS provider* means any United States person that offers any Infrastructure as a Service product.

United States person or *U.S. person* means any U.S. citizen, lawful permanent resident of the United States as defined by the Immigration and Nationality Act, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person located in the United States.

United States Reseller or *U.S. Reseller* means a reseller that is a United States person.

§ 7.302 Customer Identification Program.

(a) *In general.* Each U.S. IaaS provider of U.S. IaaS products must maintain and implement a written Customer Identification Program (CIP) that meets the requirements in this section.

(b) *Scope of CIP.* The CIP must be appropriate for the IaaS providers' size, type of IaaS products offered, and relevant risks (including those presented by the various types of service offerings maintained by the IaaS providers, the various methods of opening Accounts, the varying types of identifying information available, and the IaaS providers' customer base) that, at a minimum, include each of the requirements of this section. Any IaaS provider who is only a reseller of U.S. IaaS products, may, by agreement with the initial U.S. IaaS provider, reference, use, or adopt the initial U.S. IaaS provider's CIP for purposes of meeting the requirements of this section.

(c) *Foreign reseller CIP.* As specified in § 7.303(a), U.S. IaaS providers of U.S. IaaS products must ensure that foreign resellers of their U.S. IaaS products maintain and implement a written CIP that meets the requirements in this paragraph (c) and paragraphs (d) and (e) of this section.

(d) *Identity verification procedures.* The CIP must include risk-based procedures for verifying the identity of each foreign customer to the extent it enables the U.S. IaaS provider or foreign reseller of U.S. IaaS products to form a reasonable belief that it knows the true identity of each customer.

(1) *Customer information required.* (i) The CIP must contain procedures that enable the U.S. IaaS provider or foreign reseller of U.S. IaaS products to determine whether a potential customer and all beneficial owners are U.S. persons. If the IaaS provider determines the potential customer and all beneficial owners are U.S. persons, this subpart will not apply to any IaaS Account opened for use by that U.S. person. U.S. IaaS providers and foreign resellers of U.S. IaaS products must exercise reasonable due diligence to ascertain the true identity of any customer or beneficial owner of an Account who claims to be a U.S. person.

(ii) The CIP must contain procedures for opening an Account that specify the identifying information that will be obtained from each potential customer and beneficial owner(s) of an Account that will be used to determine whether they are U.S. persons. These procedures must 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 reflect reasonable due diligence efforts.

(iii) All U.S. IaaS providers and all of their foreign resellers of U.S. IaaS products must obtain, at a minimum, the following information from any potential foreign customer or foreign beneficial owner prior to opening an Account:

(A) Name, which shall be:

(*1*) For an individual, full legal name; or

(*2*) For an entity, business name, including all names under which the business is known to be or has been doing business.

(B) Address, which shall be:

(*1*) For an individual, a residential or business street address and the location(s) from which the IaaS product will be used.

(*2*) For an individual who does not have a residential or business street address, an Army Post Office (APO) or Fleet Post Office (FPO) box number, and the location(s) from which the IaaS product will be used.

(*3*) For an entity, a principal place of business, or if an entity is not a business, the address to which inquiries should be directed, and the location(s) from which the IaaS product will be used.

(*4*) For a person other than an individual (such as a corporation, partnership, or trust), the jurisdiction under whose laws the person is constituted or organized; and

(*5*) For a person other than an individual (such as a corporation, partnership, or trust), the name(s) of the beneficial owner(s) of that Account.

(C) Means and source of payment for the Account including:

(*1*) Credit card number;

(*2*) Account number;

(*3*) Customer identifier;

(*4*) Transaction identifier;

(*5*) Virtual currency wallet or wallet address identifier;

(*6*) Equivalent payment processing information, for alternative sources of payment; or

(*7*) Any other payment sources or types used.

(D) Email address.

(E) Telephonic contact information.

(F) internet protocol (IP) addresses used for access or administration and the date and time of each such access or administrative action, related to ongoing verification of such foreign person's ownership or control of such Account.

(2) *Customer verification.* The CIP must contain procedures for verifying the identity of the potential foreign customer and beneficial owners of the Account, including by using information obtained in accordance with paragraph (d)(1) of this section, prior to opening the Account. The procedures must include a documentary verification method, as provided in paragraph (d)(2)(i) of this section, a non-documentary verification method, as described in paragraph (d)(2)(ii) of this section or a combination of both methods.

(i) *Verification through documents.* For an IaaS provider relying on documents, the CIP must contain procedures that set forth the documents the IaaS provider will use and its method for ascertaining the documents are valid.

(ii) *Verification through non-documentary methods.* For an IaaS provider relying on non-documentary methods, the CIP must contain procedures that describe the non-documentary methods the IaaS provider will use.

(iii) *Additional verification for certain customers.* The CIP must address situations where, based on the IaaS provider's risk assessment of a new Account opened by an entity, the IaaS provider will obtain further information about individuals and beneficial owners of the Account, including signatories, in order to verify the potential customer's identity. This verification method applies only when the IaaS provider cannot verify the potential customer's identity using the verification methods described in paragraphs (d)(2)(i) and (ii) of this section or when the attempted verification leads the IaaS provider to doubt the true identity of the potential customer.

(iv) *U.S. person accounts.* If the IaaS provider verifies, through the procedures outlined in paragraphs (d)(2)(i) through (iii) of this section, that the customer and all beneficial owners are U.S. persons, the Account will not be subject to any other regulation in this subpart.

(3) *Lack of verification.* The CIP must include procedures for responding to circumstances in which the U.S. IaaS provider or foreign reseller of U.S. IaaS products cannot form a reasonable belief that it knows the identity of a customer or beneficial owner. These procedures should describe:

(i) When the IaaS provider should not open an Account for the potential customer;

(ii) The terms under which a customer may use an Account while the IaaS provider attempts to verify the identity of a customer or beneficial owner of the Account, such as restricted permission or enhanced monitoring of the Account;

(iii) When the IaaS provider should close an Account or subject it to other measures, such as additional monitoring, permitted to be used under paragraph (d)(3)(ii) of this section, after attempts to verify the identity of a customer or beneficial owner of the Account have failed; and

(iv) Other measures for account management or redress for customers whose identification could not be verified or whose information may have been compromised.

(e) *Recordkeeping.* The CIP must include procedures for making and maintaining a record of all information obtained under the procedures implementing paragraph (d) of this section.

(1) *Required records.* At a minimum, the record must include for any foreign customer or beneficial owner buying from a U.S. IaaS provider or foreign reseller of U.S. IaaS products:

(i) All identifying information about a customer or beneficial owner obtained under paragraph (d) of this section;

(ii) A copy or description of any document that was relied on under paragraph (d)(2)(i) of this section;

(iii) A description of any methods and the results of any measures undertaken to verify the identity of the customer and beneficial owners under paragraph (d)(2)(ii) or (iii) of this section; and

(iv) A description of the resolution of any substantive discrepancy discovered when verifying the identifying information obtained.

(2) *Retention of records.* U.S. IaaS providers of U.S. IaaS products must retain the records required under paragraph (e)(1) of this section for at least two years after the date the Account is closed or the date the Account was last accessed.

(3) *Limits on third-party access to records created and maintained pursuant to this subpart.* The CIP must include methods to ensure that records created and maintained pursuant to this subpart will not be shared with any third party, except insofar as such access is otherwise consistent with this subpart or lawful. Such methods should include methods to prevent unauthorized access to such records by a third party or employee of the IaaS provider without a need-to-know, including encryption and/or other methods to protect the availability, integrity, and confidentiality of such records. However, these limits need not apply when sharing security best practices or other threat information with other U.S. IaaS providers of U.S. IaaS products, or relevant consortia.

(f) *Periodic review.* The CIP must include risk-based procedures for:

(1) Requiring a customer to notify the IaaS provider when the customer adds beneficial owners to its account; and

(2) Periodic continued verification of the accuracy of the information provided by a customer.

§ 7.303 Foreign reseller requirements.

(a) *In general.* U.S. IaaS providers that contract with, enable, or otherwise allow foreign resellers to resell their

U.S. IaaS products will be subject to certain requirements. Each U.S. IaaS provider must ensure that any foreign reseller of its U.S. IaaS products maintains and implements a written CIP as specified in paragraph (b) of this section and must furnish a foreign reseller's written CIP upon request from the Department, as specified in paragraph (c) of this section.

(b) *CIP requirements.* Each U.S. IaaS provider must require that any foreign reseller of its U.S. IaaS products maintains and implements a written CIP that meets the requirements set forth in § 7.302(d) through (f).

(c) *Collecting and reporting on foreign reseller CIPs.* Each U.S. IaaS provider must follow procedures related to reporting on the implementation of CIPs for each of the U.S. IaaS provider's foreign resellers as required in § 7.304(e) and (f) and according to requirements described in § 7.304(a) through (d).

(d) *Furnishing records.* Upon receiving a request from the Department for a foreign reseller's written CIP, the U.S. IaaS provider of U.S. IaaS products must provide the foreign reseller's written CIP to the Department within ten calendar days of the Department's request.

(e) *Investigation, remediation, and termination of foreign reseller relationship.* A U.S. IaaS provider must ensure that its foreign resellers maintain CIPs that comply with the requirements set forth in § 7.302(c) through (e). A U.S. IaaS provider must, 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, take steps to close the foreign reseller account and, if relevant, to report the suspected or actual malicious cyber-enabled activity discovered to relevant authorities according to the procedures the U.S. IaaS provider has described in their CIP according to § 7.304(a)(2)(v). The U.S. IaaS provider must terminate the reseller relationship within 30 calendar days if the U.S. IaaS provider has knowledge that the foreign reseller has not remediated the issues identified or discovered by the U.S. IaaS provider, or if the continuation of the reseller relationship otherwise increases the risk its U.S. IaaS products may be used for malicious cyber-enabled activity.

§ 7.304 Customer Identification Program reporting requirements.

(a) *Certification form.* Each U.S. IaaS provider must notify the Department of implementation of its CIP and, if relevant, the CIPs of each foreign reseller of its U.S. IaaS products, through submission of a CIP certification form, which will include:

(1) A description of:

(i) The mechanisms, services, software, systems, or tools the IaaS provider uses to verify the identity of foreign persons according to criteria described in § 7.302(d);

(ii) The procedures the IaaS provider uses to require a customer to notify the IaaS provider of any changes to the customer's ownership—such as adding or removing beneficial owners—and the IaaS provider's process for ongoing verification of the accuracy of the information provided by a customer;

(iii) The mechanisms, services, software, systems, or tools used by the IaaS provider to detect malicious cyber activity;

(iv) The IaaS provider's procedures for requiring each foreign reseller to maintain a CIP;

(v) The IaaS provider's procedures for identifying when a foreign person transacts to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity, pursuant to § 7.308; and

(vi) Name, title, email, and phone number of the Primary Contact responsible for managing the CIP;

(2) Information pertaining to the IaaS provider's provision of U.S. IaaS products, including:

(i) A description of the IaaS provider's service offerings and customer bases in foreign jurisdictions;

(ii) The number of employees in IaaS provision and related services;

(iii) The mechanisms, services, software, systems, or tools used by the IaaS provider to detect malicious cyber-enabled activity, to include a description of how the mechanisms, services, software, systems, or tools are used;

(iv) The mechanisms, services, software, systems, or tools used by the IaaS provider to detect a training run that could result in the training of a large AI model with potential capabilities that could be used in malicious cyber-enabled activity;

(v) The process the IaaS provider uses to report any suspected or actual malicious cyber activity discovered to relevant authorities;

(vi) The number of IaaS customers;

(vii) The number and locations of the IaaS provider's foreign beneficial owners;

(viii) A list of all foreign resellers of IaaS products; and

(ix) The number of IaaS customer accounts held by foreign customers whose identity has not been verified, including details on:

(A) The date the IaaS provider provisioned the account, or accounts, for each customer whose identity is unverified;

(B) A description and timeline of actions the IaaS provider will take to verify the identity of each customer;

(C) Any other information available to the IaaS provider on the nature of the account, or accounts, provided to each unverified customer;

(D) The date the IaaS provider will deprovision the accounts if the identity of the customer continues to be unverified; and

(E) Steps the IaaS provider will take to ensure that foreign persons who failed to verify their identities do not reestablish new accounts; and

(3) An attestation that the written CIP of the IaaS provider meets the standards enumerated in § 7.302.

(b) *Annual certification.* U.S. IaaS providers must submit to the Department certifications of their CIPs on an annual basis and, if relevant, the CIPs of each foreign reseller of its U.S. IaaS products. Annual certifications may be submitted to the Department at any time within one year of their previous notification, but no earlier than 60 calendar days prior to that date. Annual certifications must include any updates to the information required in paragraph (a) of this section. Each annual certification must also include attestations that the IaaS provider has:

(1) Reviewed its CIP since the date of the last certification;

(2) Updated its CIP to account for any changes in its service offerings since its last certification;

(3) Updated its CIP to account for any changes in the threat landscape since its last certification;

(4) Ensured its CIP complies with this subpart since its last certification;

(5) Tracked the number of times the IaaS provider was unable to verify the identity of any customer since its last certification; and

(6) Recorded the resolution of each situation in which the IaaS provider was unable to verify the identity of a customer since its last certification.

(c) *Irregular updates.* Each U.S. IaaS provider must notify the Department if, outside of the normal reporting schedule described in paragraphs (a) and (b) of this section, a significant change in business operations or corporate structure has occurred or a material change to a CIP has been implemented, to include, for example, a material change in the documentary or non-documentary methods of identity verification or in the procedures for handling unverified accounts. Each U.S. IaaS provider must also notify the

Department when there is a change in the Primary Contact responsible for the CIP, or when there is a change in the Primary Contact responsible for managing the CIP of one of its foreign resellers.

(d) *New providers.* Prior to furnishing any foreign customer with an IaaS Account, any newly established U.S. IaaS provider must notify the Department of implementation of their CIP through submission of their CIP certification form in accordance with the requirements in paragraphs (a) through (c) of this section. U.S. IaaS providers must notify the Department according to procedures described in paragraphs (e) and (f) of this section prior to the provision of U.S. IaaS products to a new foreign reseller of its U.S. IaaS products.

(e) *Collection of information from foreign resellers.* Each U.S. IaaS provider of U.S. IaaS products must collect from its foreign resellers the information necessary for the initial and annual reporting requirements in paragraphs (a) and (b) of this section.

(f) *Reporting of information from foreign resellers.* Each U.S. IaaS provider of U.S. IaaS products must submit on an annual basis CIP certification forms for all foreign resellers' CIPs, containing the information specified in paragraph (a) of this section. Foreign reseller certifications may be submitted by the U.S. IaaS provider—in compiled format—to the Department at any time within one year of their previous notification, and no earlier than 60 calendar days prior to that date.

§ 7.305 Compliance assessments.

(a) *Government inspection.* All U.S. IaaS providers of U.S. IaaS products must maintain a written CIP and copies of the CIPs of any of their foreign resellers and must provide any copy of these CIPs to the Department within ten calendar days of a request from the Department. If upon inspection the Department finds a CIP from either a U.S. IaaS provider or their foreign reseller fails to meet the requirements in § 7.302(b) through (f), then the Department will notify the relevant IaaS provider of the specific shortcomings identified in its CIP or, if necessary, any required special measures as described in § 7.307. The IaaS provider shall then resolve the identified shortcomings within a reasonable time period, as determined by the Department, and shall resubmit its CIP for further inspection.

(b) *In general.* The Department will review information submitted to the Department in CIP certification forms and compiled foreign reseller CIP certification forms as described in § 7.304. The Department shall, at its sole discretion as to time and manner, conduct compliance assessments of U.S. IaaS providers based on the Department's own evaluation of risks associated with a given CIP, U.S. IaaS provider, or any of its foreign resellers.

(c) *Information available.* The Department will evaluate risk and conduct compliance assessments based on available information, including but not limited to:

(1) Any information provided by U.S. IaaS provider in CIP certifications;

(2) Any additional information or communications provided to the Department;

(3) Any publicly available information or communications; and

(4) Any information otherwise obtained by or made available to the Department.

(d) *Evaluating risk.* The Department shall maintain sole discretion to evaluate risks based on criteria including, but not limited to:

(1) Assessing whether the services or products of a U.S. IaaS provider or a foreign reseller are being used or are likely to be used:

(i) By foreign malicious cyber actors; or

(ii) By a foreign person to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity; or

(2) The failure of any U.S. IaaS provider of U.S. IaaS products to:

(i) Submit a CIP certification; or

(ii) Implement measures recommended by the Department as the result of a compliance assessment.

(e) *Compliance assessments.* The Department shall conduct compliance assessments of certain U.S. IaaS providers according to the Department's evaluation of risk based on information described in paragraph (b) of this section. The Department may:

(1) Conduct compliance assessments annually or as determined by the Department based on the Department's evaluation of risk of the provider's CIP;

(2) Conduct follow-up compliance assessments of providers to ensure remediation of any findings or determinations made by the Department; and

(3) Request an audit of the U.S. IaaS provider's CIP processes and procedures.

(f) *Actions.* Based on the results of compliance assessments, the Department may:

(1) Recommend remediation measures to be taken by the U.S. IaaS providers of U.S. IaaS products, including but not limited to:

(i) Measures to address any risk of U.S. IaaS products being used in support of malicious cyber activity or to train a foreign-owned large AI model with potential capabilities that could be used in malicious cyber-enabled activity; and

(ii) Any special measures the IaaS provider must take in accordance with § 7.307; and

(2) Determine to review a transaction or class of transactions of an IaaS provider according to procedures described in subpart B of this part.

§ 7.306 Customer Identification Program exemptions.

(a) *Exemptions.* The Secretary, in accordance with such standards and procedures as outlined in this section, may exempt any U.S. IaaS provider, any specific type of Account or lessee, or any specific foreign reseller of a U.S. IaaS provider's IaaS products, from the requirements of this subpart, except §§ 7.308 and 7.309. Such standards and procedures will include a finding by the Secretary that a U.S. IaaS provider, U.S. IaaS provider's foreign reseller, Account, or lessee implements security best practices to otherwise deter abuse of IaaS products.

(b) *Abuse of IaaS Products Deterrence Program for IaaS providers.* The Secretary may make a finding that an IaaS provider complies with security best practices to deter abuse of IaaS products, provided that the IaaS provider has established an Abuse of IaaS Products Deterrence Program (ADP) consistent with this paragraph (b) and has requested a finding in accordance with the procedures in paragraph (e) of this section. Such a finding exempts an IaaS provider from the CIP requirements in §§ 7.302 and 7.304. The Secretary may also make a finding that a foreign reseller of U.S. IaaS products complies with security best practices to deter abuse of IaaS products. Such a finding exempts the U.S. IaaS provider from the requirements in §§ 7.303 and 7.304 with regard to that specific foreign reseller. Each IaaS provider that offers or maintains one or more Accounts may develop, document, and implement an ADP that is designed to detect, prevent, and mitigate malicious cyber-enabled activities in connection with their Accounts and the IaaS Accounts of its foreign resellers. The ADP must be appropriate to the size and complexity of the IaaS provider and the nature and scope of its product offerings. A U.S. IaaS provider or foreign reseller ADP must include reasonable policies and procedures to:

(1) Identify relevant Red Flags for the Accounts that the IaaS provider offers or

maintains, and incorporate those Red Flags into its ADP including considering:

(i) Risk Factors such as:

(A) The types of Accounts it offers or maintains;

(B) The methods it implements for an Account to be opened;

(C) The methods it implements for an Account to be accessed;

(D) The methods it implements to monitor and assess activities related to its Accounts; or

(E) Its current or previous experiences with malicious cyber-enabled activities.

(ii) Sources of Red Flags such as:

(A) Incidents of malicious cyber-enabled activities that IaaS providers have experienced;

(B) Vulnerabilities that could contribute to malicious cyber-enabled activities if left unmitigated;

(C) Methods of malicious cyber-enabled activities that IaaS providers have identified; or

(D) Alerts, notifications, or other warnings about malicious cyber-enabled activities or improved analytic tools that the IaaS provider receives, including through engagement with the consortium under paragraph (c) of this section.

(iii) Categories of Red Flags such as:

(A) Presentation of suspicious personally identifiable information or identity evidence;

(B) Suspicious or anomalous activity detected in relation to an Account; or

(C) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible fraud or abuse conducted in association with the Account, Account compromise, a newly identified vulnerability that may impact an IaaS product offering if exploited, or identity theft in connection with Accounts serviced by the IaaS provider.

(2) Detect Red Flags that have been incorporated into the ADP, including by implementing privacy-preserving data sharing and analytics methods as feasible.

(3) Respond appropriately to any Red Flags that are detected to prevent and mitigate malicious cyber-enabled activities, which may include:

(i) Monitoring an Account for evidence of malicious cyber-enabled activities;

(ii) Contacting the customer;

(iii) Changing any passwords, security codes, or other security devices that permit access to an Account;

(iv) Reopening an Account with a new account number;

(v) Rejecting a request to open a new Account;

(vi) Closing or suspending an existing Account;

(vii) Allowing only certain trusted methods of payment;

(viii) Notifying law enforcement; or

(ix) Determining that no response or a different response is warranted under the particular circumstances.

(4) Ensure the ADP (including the relevant Red Flags) is updated regularly to reflect changes in risks to Accounts, including factors such as:

(i) The experiences of the IaaS provider with malicious cyber-enabled activities;

(ii) Changes in methods of malicious cyber-enabled activities;

(iii) Changes in methods to detect, prevent, and mitigate malicious cyber-enabled activities;

(iv) Changes in the types of accounts that the IaaS provider offers or maintains; and

(v) Changes in the business arrangements of the IaaS provider including mergers, acquisitions, alliances, joint ventures, and service provider or foreign reseller arrangements.

(5) Establish procedures for the ongoing administration of the ADP. Each IaaS provider implementing an ADP must provide for the continued administration of the ADP and must:

(i) Obtain approval of the initial written ADP from either its board of directors, an appropriate committee of the board of directors, or a designated employee at the level of senior management;

(ii) Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation, and administration of the ADP;

(iii) Train staff, as necessary, to effectively implement the ADP; and

(iv) Exercise appropriate and effective oversight of reseller arrangements with respect to detecting and mitigating Red Flags.

(c) *Public-private sector collaboration.* One factor to be considered by the Department in granting an exemption is the participation of U.S. IaaS providers or a foreign reseller of U.S. IaaS products in a consortium to develop and maintain privacy-preserving data sharing and analytics to enable improved detection and mitigation of malicious cyber-enabled activities. Before implementing privacy-preserving data sharing and analytics, IaaS providers may initially evaluate solutions in a test environment which may be established and maintained by either industry or the Federal Government. The consortium will make available tools and expertise to assist smaller IaaS providers with conducting privacy-preserving data sharing and analytics, as well as providing insights, policies, and practices for improving their ADPs under paragraph (a) of this section. IaaS providers must document their process and capabilities for integrating insights and responding to intelligence generated through consortium interaction within their ADP as described in paragraph (a) of this section.

(d) *Investigative cooperation.* One factor to be considered by the Department in granting an exemption is voluntary cooperation with law enforcement, consistent with otherwise applicable law, to provide forensic information for investigations of identified malicious cyber-enabled activities.

(e) *Procedures for requests for exemptions from CIP requirements.* In consultation with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, or, as the Secretary deems appropriate, the heads of other executive departments and agencies, the Secretary may make a finding exempting a U.S. IaaS provider from the requirements in §§ 7.302, 7.304, and 7.305 if the finding determines that the U.S. IaaS provider complies with security best practices to otherwise deter the abuse of IaaS products. In consultation with these same agencies, the Secretary may also make a finding to exempt a U.S. IaaS provider with respect to any specific foreign reseller of their services from the requirements in §§ 7.303 and 7.304, if the finding determines that the foreign reseller, account, or lessee complies with security best practices to otherwise deter abuse of United States IaaS products.

(1) Any U.S. IaaS provider of U.S. IaaS products seeking to obtain the Secretary's finding exempting it or one of its foreign resellers from CIP requirements shall initiate the process by providing a written submission to the Secretary describing its establishment of an ADP consistent with paragraph (a) of this section. Such submission should be made electronically.

(2) Upon receipt of a written submission, the Secretary will review the submission and may request additional information from the submitter. Prior to making a finding, the Secretary will consult with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, or their designees.

(3) The Secretary will make a finding based on an evaluation of the following factors:

(i) Whether the ADP is an appropriate size and complexity commensurate with the nature and scope of product offerings;

(ii) Whether the Program's ability to deter, detect, and respond to Red Flags is sufficiently robust;

(iii) Whether oversight of reseller arrangements is effective;

(iv) The extent of cooperation by providers with law enforcement, consistent with otherwise applicable law, to provide forensic information for investigations of identified malicious cyber-enabled activities; and

(v) Whether they participate in public-private collaborative efforts as described in paragraph (c) of this section.

(f) *Maintenance of exemption.* U.S. IaaS providers of U.S. IaaS products have a continuing obligation to update their ADPs in response to the changing threat landscape and must notify the Secretary of any significant deviations or changes to their ADP. U.S. IaaS providers must also require their foreign resellers to do the same. All U.S. IaaS providers must provide information on such updates by submitting annual notifications for themselves or any of their exempt foreign resellers to the Department to ensure that exemptions from the CIP requirements continue to be warranted.

(g) *Revocation of exemption.* The exemption from CIP requirements may be revoked at any time, including to impose special measures as described in § 7.307.

§ 7.307 Special measures for certain foreign jurisdictions or foreign persons.

(a) *International counter-malicious cyber-enabled activity requirements*—(1) *In general.* The Secretary may require U.S. IaaS providers of U.S. IaaS products to take either of the special measures described in paragraph (b) of this section if the Secretary determines that reasonable grounds exist for concluding that a foreign jurisdiction or foreign person is conducting malicious cyber-enabled activities using U.S. IaaS products, in accordance with paragraph (c) of this section.

(2) *Evaluation.* If the Secretary, based on the Secretary's own initiative or upon referral from other executive departments and agencies or U.S. IaaS providers, is informed that reasonable grounds may exist to apply special measures to a particular foreign jurisdiction or foreign person, the Secretary will evaluate the relevant factors provided in paragraph (b) of this section and consult with the heads of other agencies as appropriate, to determine whether to impose either of the special measures described in paragraph (b), and which special measure the Secretary will impose.

(3) *Determination.* Upon completion of the evaluation, the Secretary shall issue an unclassified written determination that summarizes the elements of the evaluation. The determination shall identify whether the Secretary established, through the investigation, that reasonable grounds exist to determine that:

(i) A foreign jurisdiction has any significant number of foreign persons offering U.S. IaaS products that are used for malicious cyber-enabled activities or any significant number of foreign persons directly obtaining U.S. IaaS products for use in malicious cyber-enabled activities; or

(ii) A foreign person has established a pattern of conduct of offering U.S. IaaS products that are used for malicious cyber-enabled activities or directly obtaining U.S. IaaS products for use in malicious cyber-enabled activities.

(4) *Special measure.* The determination shall also explain how it is consistent with the terms of Executive Order 13984 and this subpart. The special measure will be imposed as soon as the Secretary issues the determination.

(5) *Duration of special measure.* Any determination by which a special measure described in paragraphs (b)(1) and (2) of this section is imposed may not remain in effect for more than 365 calendar days, except pursuant to the publication in the **Federal Register**, on or before the end of the 365-day period beginning on the date of the issuance of such determination, of a notice of extension finding that the measure remains necessary for an additional period of time.

(6) *Effective date.* No U.S. IaaS providers shall be required to take any of the special measures adopted pursuant to this section earlier than 180 calendar days following the issuance of determinations.

(7) *No limitation on other authorities.* This section shall not be construed as superseding or otherwise restricting any other authorities granted to the Secretary, or to any other agency, by this subpart or otherwise.

(b) *Special measures.* The special measures referred to in paragraph (a) of this section, with respect to a foreign jurisdiction or foreign person, are as follows:

(1) *Prohibitions or conditions on customers, potential customers, or accounts within certain foreign jurisdictions.* The Secretary may prohibit or impose conditions on the opening or maintaining with any U.S. IaaS provider of an Account, including a Reseller Account, by any foreign person located in a foreign jurisdiction found to have any significant number of foreign persons offering U.S. IaaS products used for malicious cyber-enabled activities, or by any U.S. IaaS provider of U.S. IaaS products for or on behalf of a foreign person.

(2) *Prohibitions or conditions on certain foreign persons.* The Secretary may prohibit or impose conditions on the opening or maintaining of an Account, including a Reseller Account, by any U.S. IaaS provider of U.S. IaaS products for or on behalf of a foreign person, if such an Account involves any such foreign person found to be directly obtaining or engaged in a pattern of conduct of obtaining U.S. IaaS products for use in malicious cyber-enabled activities or offering U.S. IaaS products used in malicious cyber-enabled activities.

(3) *Reasonable grounds determination factors.* In making a determination described in paragraph (a) of this section, the Secretary shall consider, in addition to any and all such information as the Secretary determines to be relevant, the following potentially relevant factors:

(i) *Factors related to a particular foreign jurisdiction.* (A) Evidence that foreign malicious cyber actors have obtained U.S. IaaS products from persons offering U.S. IaaS products in that foreign jurisdiction, including whether such actors obtained such U.S. IaaS products through foreign resellers;

(B) The extent to which that foreign jurisdiction is a source of malicious cyber-enabled activities; and

(C) Whether the United States has a mutual legal assistance treaty with that foreign jurisdiction, and the experience of law enforcement officials and regulatory officials in obtaining information about activities involving U.S. IaaS products originating in or routed through such foreign jurisdiction.

(ii) *Factors related to a particular foreign person.* (A) The extent to which a foreign person uses U.S. IaaS products to conduct, facilitate, or promote malicious cyber-enabled activities;

(B) The extent to which U.S. IaaS products offered by a foreign person are used to facilitate or promote malicious cyber-enabled activities;

(C) The extent to which U.S. IaaS products offered by a foreign person are used for legitimate business purposes in the foreign jurisdiction; and

(D) The extent to which actions short of the imposition of special measures pursuant to this paragraph (b) are sufficient, with respect to transactions

involving the foreign person offering U.S. IaaS products, to guard against malicious cyber-enabled activities.

(4) *Special measure determination factors.* In selecting which special measure(s) to take under this section, the Secretary shall consider:

(i) Whether the imposition of any special measure would create a significant competitive disadvantage, including any undue cost or burden associated with compliance, for U.S. IaaS providers;

(ii) The extent to which the imposition of any special measure(s) or the timing of any special measure(s) would have a significant adverse effect on legitimate business activities involving the particular foreign jurisdiction or foreign person; and

(iii) The effect of any special measure(s) on United States national security, law enforcement investigations, U.S. supply chains, foreign policy, or any serious effect on U.S. public health or safety.

(c) *Consultations and information to be considered in finding foreign jurisdictions or foreign persons to be of primary malicious cyber-enabled activity concern.* In general, in making a determination described in paragraph (a) of this section, the Secretary shall consult with the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of National Intelligence, and, as the Secretary deems appropriate, the heads of other executive departments and agencies.

(d) *Notification of special measures invoked by the Secretary.* Not later than 10 calendar days after the date of any determination under paragraph (a)(4) of this section, the Secretary shall notify, in writing, the Committee on Energy and Commerce of the U.S. House of Representatives and the Committee on Commerce, Science, and Transportation of the U.S. Senate of any such action.

§ 7.308 Reporting of large AI model training.

(a) *Reporting requirements.* (1) In general, each U.S. IaaS provider must submit a report to the Department whenever they have ''knowledge'' of a covered transaction, as specified in paragraph (b) of this section, at the time specified in paragraph (c) of this section.

(2) Each U.S. IaaS provider must also require that their foreign resellers submit a report whenever they have ''knowledge'' of a covered transaction, as specified in paragraph (b) of this section, at the time specified in paragraph (c) of this section to the U.S. IaaS provider.

(3) Reports must be submitted to the Department in the form and manner specified in paragraph (d) of this section and, at a minimum, include responses for each of the requirements of paragraphs (d)(1)(i) through (ii) of this section.

(b) *Covered transactions.* (1) Transactions that are covered transactions for the purposes of this section include:

(i) A transaction by, for, or on behalf of a foreign person which results or could result in the training of a large AI model with potential capabilities that could be used in malicious cyber-enabled activity (see the examples in paragraphs (b)(3)(i) and (ii) of this section); or

(ii) A transaction by, for, or on behalf of a foreign person, in which the original arrangements provided for in the terms of the transaction would not result in a training of a large AI model with potential capabilities that could be used in malicious cyber-enabled activity, but a development or update in the arrangements means the transaction now does or could result in the training of a large AI model with potential capabilities that could be used in malicious cyber-enabled activity (see the example in paragraph (b)(3)(iii) of this section).

(2) A model shall be considered to be a large AI model with potential capabilities that could be used in malicious cyber-enabled activity under the definition provided in § 7.301 if it meets the requirements laid out by the Department in interpretive rules published in the **Federal Register**.

(3)(i) *Example 1.* Corporation A, a foreign person, proposes to train a model on the computing infrastructure of Corporation B, a U.S. IaaS provider, and signs an agreement with Corporation B to train the proposed model. The technical specifications of the model that Corporation A seeks to train meet the technical conditions of a large AI model with potential capabilities that could be used in malicious cyber-enabled activity. The transaction is a covered transaction.

(ii) *Example 2.* Corporation A, a U.S. person, makes an equity investment in Corporation B, a foreign person, and a portion of that investment is in the form of credits to use Corporation A's computing infrastructure. Corporation A has reason to believe that Corporation B intends to use those credits to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity. The transaction is a covered transaction.

(iii) *Example 3.* Corporation A, a U.S. person, agrees to train an AI model for Corporation B, a foreign person. At the outset, the agreed-upon technical specifications for the model do not meet the technical conditions of a dual-use foundation model or a model with technical conditions of concern. However, after training commences, adjustments in the training procedure or new insights about the model's capabilities provide Corporation A with reason to believe that the model will in fact have the technical conditions of a large AI model with potential capabilities that could be used in malicious cyber-enabled activity. The transaction becomes a covered transaction.

(iv) *Example 4.* Corporation A, a U.S. person, agrees to train an AI model for Corporation B, a foreign person, on a computing infrastructure co-located in a facility owned by Corporation C. The model will have the technical conditions of a large AI model with potential capabilities that could be used in malicious cyber-enabled activity. The transaction is a covered transaction, and Corporation A is responsible for reporting the training run to the Department.

(c) *Timing of reports*—(1) *Initial U.S. IaaS provider report.* U.S. IaaS providers shall file with the Department a report within 15 calendar days of a covered transaction occurring or the provider or reseller having ''knowledge'' that a covered transaction has occurred.

(2) *Initial foreign reseller report.* U.S. IaaS providers must require their foreign resellers to file with the U.S. IaaS provider a report within 15 calendar days of a covered transaction occurring or the provider or reseller having ''knowledge'' that a covered transaction has occurred. The U.S. IaaS provider must file this report with the Department within 30 calendar days of the covered transaction.

(3) *Follow-up report.* Any U.S. IaaS provider that receives a request from the Department for additional information, as outlined in paragraph (d) of this section, whether in regard to a covered transaction of itself or its foreign reseller, will file a follow-up report responsive to the request within 15 calendar days of receiving the request for additional information.

(4) *Corrected report.* If any report filed under this section is found to have been inaccurate when filed, the U.S. IaaS provider shall file a corrected report in the form and manner specified in paragraph (d) of this section within 15 calendar dates after the date on which the U.S. IaaS provider has ''knowledge'' of the inaccuracy.

(d) *Content, form, and manner of reports.* Each report submitted under this section shall be filed with the Department in the form and manner that the Department shall prescribe in the forms and instructions for such report, and each person filing such report shall certify that the report or application is true, correct, and complete.

(1) *Initial U.S. IaaS provider and foreign reseller report.* An initial report of an IaaS provider shall include the following:

(i) *Information about the foreign person.* (A) Name of the foreign customer or foreign beneficial owner of the customer, which shall be:

(*1*) For an individual, full legal name; or

(*2*) For an entity, business name, including all names under which the business is known to be or has been doing business.

(*3*) For both individuals and entities, the ultimate beneficial owner, if it is not the same as the individual or entity.

(B) Address, which shall be:

(*1*) For an individual, a residential or business street address.

(*2*) For an individual who does not have a residential or business street address, an Army Post Office (APO) or Fleet Post Office (FPO) box number.

(*3*) For an entity, principal places of business, or if an entity is not a business, the address to which inquiries should be directed, and the location(s) from which the training request originates.

(*4*) For a person other than an individual (such as a corporation, partnership, or trust), the jurisdiction under whose laws the person is constituted or organized; and

(*5*) For a person other than an individual (such as a corporation, partnership, or trust), the name(s) of the beneficial owner(s) of that account, including the ultimate beneficial owner(s).

(C) Means and source of payment for the account including:

(*1*) Credit card number;

(*2*) Account number;

(*3*) Customer identifier;

(*4*) Transaction identifier;

(*5*) Virtual currency wallet or wallet address identifier;

(*6*) Equivalent payment processing information, for alternative sources of payment; or

(*7*) Any other payment sources or types used.

(D) Email address.

(E) Telephonic contact information.

(F) IP addresses used for access or administration and the date and time of each such access or administrative action, related to ongoing verification of such foreign person's ownership or control of such Account.

(ii) *Information about the training run.* (A) Estimated number of computational operations (*e.g.,* integer operations or floating-point operations) used in the training run.

(B) Anticipated start date and completion date of the training run.

(C) Information on training practices, including the model of the primary AI used in the training run accelerators.

(D) Information on cybersecurity practices including:

(*1*) Policies and procedures for ensuring secure storage of, and protecting access to, trained model weights; and

(*2*) Any cybersecurity or insider threat events that have occurred in the last four years that have resulted in unauthorized access to model weights or model source code, or other damages of major concern.

(2) *Follow-up report.* A follow-up report filed pursuant to a request for additional information in paragraph (c) of this section shall include all information responsive to the request.

(3) *Corrected report.* A corrected report required to be filed pursuant to paragraph (c) of this section shall correct all inaccuracies in the information previously reported to BIS.

(e) *Request for additional information.* Upon receiving an initial report, follow-up report, or corrected report, BIS may request that a U.S. IaaS provider or foreign reseller of U.S. IaaS products submit additional information pertaining to activities or risks that present concerns to U.S. national security.

(f) *Prohibition.* No U.S. IaaS provider shall provide U.S. IaaS products to foreign resellers, unless the U.S. IaaS provider has made all reasonable efforts to ensure that the foreign reseller complies with the requirements of this section. Upon receipt of evidence, or upon discovery of facts and circumstances that indicate that a foreign reseller has not complied with the requirements of this section, the U.S. IaaS provider shall notify the foreign reseller of the alleged violation and request written confirmation and supporting evidence of compliance, remediation, or both. Upon subsequent receipt of evidence, or discovery of facts and circumstances that indicate the foreign reseller did not remediate, or remains out of compliance, the U.S. IaaS provider must suspend the provision of U.S. IaaS products to the foreign reseller, and shall resume provision of U.S. IaaS products only after the foreign reseller has provided adequate assurances to prevent future violations.

§ 7.309 Enforcement.

(a) *Prohibitions.* The following are prohibited:

(1) Engaging in, or conspiring to engage in, any conduct prohibited by the regulations issued in this part.

(2) Failing to submit reports, certifications, or recertifications, as appropriate, or failing to comply with terms of notices or orders provided by the Department, and as required by this subpart.

(3) Failing to implement or maintain CIPs as required by § 7.302, or continuing to transact with a foreign reseller that fails to implement or maintain a CIP as set forth in § 7.303.

(4) Providing IaaS products to a foreign person while failing to comply with any direction, determination, or condition issued under this part.

(5) Aiding, abetting, counseling, commanding, inducing, procuring, permitting, approving, or otherwise supporting any act prohibited by any direction, determination, or condition issued under this part.

(6) Attempting or soliciting a violation of any direction, determination, or condition issued under this part.

(7) Failing to implement any prohibition or suspension as set forth in § 7.308.

(8) Making a false or misleading representation, statement, notification, or certification, whether directly or indirectly through any other person, or falsifying or concealing any material fact to the Department in connection with compliance under this part.

(b) *Additional obligations.* (1) Any person who makes a representation, statement, or certification to the Department relating to the creation or maintenance of a CIP, reporting required under the CIP, in a written request for an exemption, an annual notification related to exemptions, or in relation to their own or another entities ADP shall notify the Department of any material change to the CIP or to the IaaS provider's business, that renders the CIP unnecessary.

(2) Any person who has been granted, or has had a foreign reseller granted, an exemption on the basis of their ADP shall notify the Department of any material change to the ADP or to the IaaS provider's business that may impact the ADP.

(3) For purposes of paragraph (a)(8) of this section, any representation, statement, or certification, such as (though not limited to) CIPs, written request for exemption, or written statements on ADPs made by any person shall be deemed to be continuing in effect until the person notifies the

Department in accordance with this part.

(c) *Maximum penalties*—(1) *Civil penalty.* A civil penalty not to exceed the amount set forth in section 206 of IEEPA, 50 U.S.C. 1705, may be imposed on any person who violates, attempts to violate, conspires to violate, or knowingly causes any violation of paragraph (a) of this section. IEEPA provides for a maximum civil penalty not to exceed the greater of $250,000 per violation, subject to inflationary adjustment, or an amount that is twice the amount of the transaction that is the basis of the violation with respect to which the penalty is imposed.

(i) Notice of the penalty, including a written explanation of the penalized conduct specifying the laws and regulations allegedly violated and the amount of the proposed penalty, and notifying the recipient of a right to make a written petition within 30 calendar days as to why a penalty should not be imposed, shall be served on the notified party or parties.

(ii) The Secretary shall review any presentation and issue a final administrative decision within 30 calendar days of receipt of the petition.

(2) *Criminal penalty.* A person who willfully commits, attempts to commit, or conspires to commit, or aids and abets in the commission of a violation of paragraph (a) of this section shall, upon conviction of a violation of IEEPA, be fined not more than $1,000,000, or if a natural person, may be imprisoned for not more than 20 years, or both.

(3) *Civil penalty recovery.* Any civil penalties authorized in this section may be recovered in a civil action brought by the United States in U.S. district court.

(d) *Adjustments to penalty amounts.* (1) The civil penalties provided in IEEPA are subject to adjustment pursuant to the Federal Civil Penalties Inflation Adjustment Act of 1990 (Pub. L. 101–410, as amended, 28 U.S.C. 2461 note).

(2) The criminal penalties provided in IEEPA are subject to adjustment pursuant to 18 U.S.C. 3571.

(e) *Other penalities.* The penalties available under this section are without prejudice to other penalties, civil or criminal, available under law. Attention is directed to 18 U.S.C. 1001, which provides that whoever, in any matter within the jurisdiction of any department or agency in the United States, knowingly and willfully falsifies, conceals, or covers up by any trick, scheme, or device a material fact, or makes any false, fictitious, or fraudulent statements or representations, or makes or uses any false writing or document knowing the same to contain any false, fictitious, or fraudulent statement or entry, shall be fined under title 18, United States Code, or imprisoned not more than 5 years, or both.

§ 7.310 Reporting violations.

(a) *Where to report.* If a person learns of facts or circumstances that indicate a violation of any of the requirements in this subpart may have occurred, or are likely to occur, that person may notify: Office of Information and Communications Technology and Services, Bureau of Industry and Security, U.S. Department of Commerce, 14th Street and Constitution Avenue NW, Room A–100, Washington, DC 20230.

(b) *Reporting distinguished.* The reporting provisions in paragraph (a) of this section are not the ''reporting of violations'' contained within the Export Administration Regulations (EAR) in 15 CFR chapter VII, subchapter C, nor the ''voluntary self-disclosure'' within the same.

Alan F. Estevez,

Under Secretary of Commerce for Industry and Security, U.S. Department of Commerce.

[FR Doc. 2024–01580 Filed 1–26–24; 8:45 am]

BILLING CODE 3510–20–P