: 3510-20

DEPARTMENT OF COMMERCE

15 CFR Subtitle A

[210913-0183]

RIN 0605-AA61

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

AGENCY: U.S. Department of Commerce.

ACTION: Advance notice of proposed rulemaking (ANPRM).

SUMMARY: Executive Order 13984 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 implement regulations to govern the process and procedures that the Secretary will use to deter foreign malicious cyber actors' use of United States Infrastructure as a Service (IaaS) products and assist in the investigation of transactions involving foreign malicious cyber actors. The Department of Commerce (the Department) is issuing this ANPRM to solicit public comments on questions pertinent to the development of regulations pursuant to this ExecutiveOrder.

DATES: Comments must be received by [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

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

- *By the Federal eRulemaking Portal: http://www.regulations.gov* at docket number: DOC-2021-0007.
- *By email directly to: IaaScomments@doc.gov.* Include "E.O. 13984: ANPRM" 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: Justin LP Shore, U.S. Department of Commerce, email: IaaScomments@doc.gov. For media inquiries: Brittany Caplin, Deputy Director of Public Affairs and Press Secretary, U.S. Department of Commerce, telephone: (202) 482-4883, email: PublicAffairs@doc.gov.

SUPPLEMENTARY INFORMATION:

I. Background

E.O. 13984, issued on January 19, 2021, and entitled "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities,"[1] was issued pursuant to the President's authority under the Constitution and the laws of the United States, including the International Emergency Economic Powers Act,[2] the National Emergencies Act,[3] and section 301 of Title 3, United States Code. In EO 13984, the President determined that additional steps must be taken to address the national emergency related to significant malicious cyber-enabled activities declared in Executive Order 13694, *Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities* (80 FR 18077, Apr. 1, 2015).

E.O. 13984 addresses the threat posed by the use of U.S. cloud infrastructure by foreign

[1] E.O. 13984, 86 FR 6837 (Jan. 19, 2021).
[2] Pub.L. 95-223 (October 28, 1977), 91 Stat. 1626, codified as amended at 50 U.S.C. 1701 et seq. (2018) ("IEEPA").
[3] Pub.L. 94-412 (September 14, 1976), 90 Stat. 1255, codified as amended at 50 U.S.C. 1601 et seq. (2018) ("NEA").

malicious cyber actors to conduct malicious cyber-enabled activities, including theft of sensitive data and intellectual property and targeting of U.S. critical infrastructure. IaaS products provide the ability to run software and store data on servers offered for rent or lease without responsibility for the maintenance and operating costs of those servers.[4] The United States must ensure that providers offering United States IaaS products verify the identity of persons obtaining an IaaS account for the provision of these products and maintain records of those transactions[5] as foreign persons obtain or offer for resale IaaS accounts (Accounts) with U.S. IaaS providers, and then use these Accounts to conduct malicious cyber-enabled activities against U.S. interests. Malicious actors then destroy evidence of their prior activities and transition to other services. This pattern makes it extremely difficult to track and obtain information on foreign malicious cyber actors and their activities in a timely manner, especially if U.S. IaaS providers do not maintain updated information and records of their customers or the lessees and sub-lessees of those customers.

To "deter foreign malicious cyber actors' use of U.S. IaaS products, and assist in the investigation of transactions involving foreign malicious cyber actors,"[6] E.O. 13984 requires more robust record-keeping practices and user identification and verification standards within the industry to better assist investigative efforts. Additionally, E.O. 13984 encourages the adoption of and adherence to security best practices to deter abuse of U.S. IaaS products by allowing the Secretary to take into account compliance with such best practices in deciding to exempt certain U.S. IaaS providers, Accounts, or lessees from any final regulations stemming from Section 1 of E.O. 13984.

E.O. 13984 tasks the Secretary, specifically, with implementing regulations that require U.S. IaaS providers to: 1) verify the identity of a foreign person that obtains an Account (i.e. identification, verification, and recordkeeping obligations) (Section 1); and 2) implement special

---

[4] E.O. 13984 at 6837.
[5] *Id.*
[6] *Id*.

measures to prohibit or impose conditions on Accounts within certain foreign jurisdictions or of certain foreign persons, where the Secretary, in consultation with specified agency heads, makes a finding that either i) reasonable grounds exist for concluding that a foreign jurisdiction has any significant number of foreign persons offering U.S. IaaS products, as defined in Section 5 of E.O. 13984, 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) reasonable grounds exist for concluding that 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 (Section 2). Section 3 of E.O. 13984, which is not a part of this potential rulemaking, directs the Attorney General and the Secretary of Homeland Security, in coordination with the Secretary and the heads of other agencies, as deemed appropriate, to solicit feedback from industry that culminates in a report to the President recommending ways to encourage information sharing and collaboration amongst U.S. IaaS providers and government. Finally, Sections 4-7 consider resources necessary for implementation, relevant definitions, reporting authorizations, and other general provisions. This ANPRM seeks comments specifically on how the Secretary should implement, through regulation, E.O. 13984 Section 1 (*Verification of Identity*), Section 2 (*Special Measures for Certain Foreign Jurisdictions or Foreign Persons*), and Section 5 (*Definitions*).

II. Issues for Comment

The Department welcomes comments and views on all aspects of how the Secretary should implement Sections 1, 2, and 5 of E.O. 13984, but is particularly interested in obtaining information on the following questions, within four categories: 1) customer due diligence regulations and relevant exemptions; 2) special measures; 3) definitions, and 4) overarching inquiries. The Department encourages commenters to reference specific question numbers to

facilitate the Department's review of comments.

Customer Due Diligence Regulations and Relevant Exemptions:

1) E.O. 13984 requires the Secretary to promulgate regulations that set forth minimum standards that U.S. IaaS providers must adopt to verify the identity of a foreign person when 1) opening an Account or 2) "maintain[ing]" an existing Account, including types of documentation and procedures required for verification and records that U.S. IaaS providers must securely maintain in both instances.
    a. How should the Department implement the requirement for both verifying a foreign person's identity 1) upon the opening of an Account, and 2) during the "maintenance of an existing Account," and what should the Department consider in determining customer due diligence requirements for U.S. IaaS providers?
    b. Can the Department implement the requirement to verify a foreign person's identity 1) upon the opening of an Account, and 2) during the "maintenance of an existing Account," while minimizing the impact on U.S. persons' opening or using such Accounts, or will the application of the requirements to foreign persons in practice necessitate the application of that requirement across all customers?
    c. How do the records specifically identified within Section 1(a)(ii)(A)-(D) compare with the types of customer documentation and records that are currently collected by U.S. IaaS providers? Will changes be required in U.S. IaaS providers' business processes or technical architectures for the maintenance of the records explicitly listed in Section 1(a)(ii)(A)-(D), and if so, what are these changes? What differences may exist in U.S. IaaS

providers' ability to obtain certain records based on the type of U.S. IaaS product in question (i.e. managed vs. unmanaged services, virtual private servers or virtual private network products vs. cloud services)? What level of burden for U.S. IaaS providers would be associated with such changes?

d. Do U.S. IaaS providers currently collect information on the true users of their respective IaaS products, to include reselling activities? If no, what level of burden would be associated with a requirement to track lessees through resellers, including to verify nationality and collect/store identity information, and to augment existing U.S. IaaS providers' Terms and Conditions and Service Level Agreements to reflect these obligations?

e. What additional identifying information is collected by U.S. IaaS providers that could potentially assist with verification of customer identity and customer due diligence? Do U.S. IaaS providers possess other categories of information that would assist in the identification and investigation of foreign malicious cyber actors (e.g., Account log information, suspicious/abnormal Account activity reports, threat monitoring reports, suspended or blocked services by third parties, etc.)? What would be the associated benefits or costs of including such records within the scope of the obligation to maintain records of foreign persons that obtain an Account?

f. Do U.S. IaaS providers have the capacity or capability to augment technical identity verification (e.g., Two-Factor Authentication (2FA)) with additional, non-technical vetting (e.g., third-party person/entity vouching) to further deter foreign malicious cyber actors from acquiring replacement infrastructure?

g. What types of data or technical analyses, if any, do U.S. IaaS providers

use to identify or detect accounts that violate terms of service related to identify verification—including for those using fake names, fraudulent government documents or other fraudulent identification records—of relevant services?

h. What procedures and processes should the Department consider to minimize the potential burden on U.S. IaaS providers to implement verification and recordkeeping obligations under E.O. 13984?

i. Do U.S. IaaS providers currently take a risk-based approach to customer verification and ongoing customer due diligence, and should the Department consider some form of blended risk-based approach (i.e., a small number of explicitly listed minimum identification and verification requirements, coupled with a more risk-based approach to allow providers to develop their own programs based on their specific operations)?

j. What should the Department consider, including U.S. IaaS providers' current methods of securing and limiting access to personally identifiable information and other sensitive data, when setting forth minimum standards and methods by which U.S. IaaS providers should limit third-party access to the records that are described in Section 1(a)(ii)(A)-(D), or that might otherwise be required to be maintained?

2) What data protection and security implications should the Department be aware of when considering the imposition on U.S. IaaS providers of requirements to maintain records regarding foreign person customers? For example, how might the European Union General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), or other relevant data protection and security laws and regulations affect U.S. IaaS providers' ability to fulfill these record-keeping requirements pursuant to E.O. 13984? Should the Department consider

specific limitations on the amount of time that such records must be kept?

3) What other international implications for U.S. IaaS providers should the Department be aware of when designing customer due diligence rules? How can the Department mitigate the risk of negative international consequences, if any, of such rules?

4) What should the Department consider when deciding how compliance with the requirements adopted under Section 1 should be monitored and enforced (i.e., should compliance and enforcement be strictly limited to instances following malicious cyber activities that are traced back to specific U.S. IaaS providers; should the Department implement a voluntary or required proactive suspicious/abnormal Account activity report mechanism to assist in ongoing due diligence; should the Department periodically conduct compliance audits)? How should the Department verify that Section 1 requirements are being met?

5) Section 1(c) permits the Secretary, in consultation with other Federal agency heads, to provide an exemption from the requirements of any rules issued pursuant to Section 1 to a "provider, Account, or lessee [that] complies with security best practices to otherwise deter abuse of IaaS products."[7]

    a. Should exemptions be granted on a one-time basis, or should such exemptions be time-limited, with an obligation of renewal after a certain period of time? If renewals are required, what should be the timeframe for renewals?

    b. What security practices do U.S. IaaS providers currently use to identify or detect foreign malicious cyber actors' abuse of their services?

    c. What IaaS industry standards or best practices should the Department use to assess the appropriateness of an exemption from the rules issued under

[7] EO 13984 at 6838.

Section 1? To what extent are these standards or best practices sufficient to deter abuse of U.S. IaaS products by foreign malicious cyber actors? Would existing standards or practices need to be adapted for purposes of E.O. 13984?

d. How might a framework for best practices account for the dynamic and ever-evolving threat environment while allowing U.S. IaaS providers to stay agile in their company-specific programs?

e. How should the Secretary assess compliance with any security best practices for purposes of determining whether an exemption should be granted for a U.S. IaaS provider, type of account, or type of lessee? Should U.S. IaaS providers be permitted to conduct a self-assessment of such compliance, and if so, what type of documentation or certification should be required? Should verification of compliance by an independent third-party be required? If so, what should be assessed by that third party and what documentation should the Secretary request?

f. When granting exemptions, should the Secretary consider granting partial exemptions from the rules issued under Section 1 (i.e., should the Secretary consider exempting certain providers, types of Accounts, or types of lessees from initial customer due diligence verification procedures, but *not* any ongoing customer-due-diligence procedures)?

g. What should the Department take into consideration when determining if specific "types" of Accounts or lessees should be exempt from Section 1 rules?

Special Measures Restrictions:

Section 2 permits the Secretary, in consultation 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, to require U.S. IaaS providers to implement special measures to prohibit or impose conditions on Accounts upon a finding that reasonable grounds exist for concluding that either: 1) certain foreign persons have established a pattern of offering or directly obtaining U.S. IaaS products that are used for malicious cyber-enabled activities; or 2) certain foreign jurisdictions have any significant number of foreign persons offering or directly obtaining U.S. IaaS products that are used for malicious cyber-enabled activities.

6) Is there particular information or sources of information that the Secretary should consider when making a determination under Section 2?
7) Form of Finding: should the Secretary be required to publish a finding in a particular form (i.e. order, regulation, etc.), and if so, what reasoning supports that form?
8) Duration of Finding: What, if any, suggested restrictions should there be regarding the duration of any special measure? Should the form of a particular finding vary depending on the special measure duration?
9) In making a reasonable grounds finding under Section 2, the E.O. requires the Secretary to consider any information the Secretary determines to be relevant, but also weigh specific, enumerated factors articulated within Section 2(b) of E.O. 13984, depending on whether the special measures pertain to a foreign jurisdiction or a foreign person. Are the factors enumerated within Section 2(b) comprehensive, or should the Secretary consider other factors when making a finding?
10) In selecting which special measure or measures to take, Section 2(c) of the E.O. requires the Secretary to 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 or the timing of the special measure 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 on U.S. national security, law enforcement investigations, or foreign policy.

a. Could the Secretary's selection of types of conditions to impose under Section 2 effectively mitigate any competitive disadvantages to U.S. IaaS providers or effects on legitimate business purposes? If so, how?

b. Are there any examples or frameworks that the Secretary should draw on in considering the factors listed in Section 2(c) (i.e., in balancing any competitive disadvantage or impact on legitimate business activities against the impact of special measures on national security and law enforcement considerations)?

11) Section 2(d) articulates the two specific special measures that the Secretary is able to take to condition or prohibit the opening or maintaining of Accounts by 1) foreign persons within certain foreign jurisdictions or by 2) certain foreign persons seeking to open or maintain an Account in the U.S.

a. Section 2(d)(i), *Prohibitions or Conditions on Accounts within Certain Foreign Jurisdictions*, permits the Secretary to prohibit or impose conditions on the opening or maintaining of an 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.[8] When implementing this provision, should the Secretary consider using this provision to impose conditions or

[8] EO 13984 at 6839.

prohibitions on specific foreign persons located within foreign jurisdictions based on findings related to the jurisdiction? What should the Secretary consider in determining whether to impose conditions or prohibitions on all foreign persons located within the foreign jurisdiction in question or only specific foreign persons or Accounts?

i. How do U.S. IaaS providers expect to implement this special measure?

ii. How are providers able to assess and verify the jurisdiction from which persons are based? What tools are available to U.S. IaaS providers to assess or verify the jurisdiction from which persons are located?

b. Section 2(d)(ii), *Prohibitions or Conditions on Certain Foreign Persons*, permits the Secretary to prohibit or impose conditions "on the opening or maintaining in the United States of an Account, including a Reseller Account, by any United States IaaS provider for or on behalf of a foreign person," if such an Account involves any such foreign person found to be offering or obtaining U.S. IaaS products for malicious cyber-enabled activities.[9] In implementing this provision, how should the Department assess whether an Account is "opened or maintained in the United States"? For example, should the Department look only at the customer's location or also at the location of the services or infrastructure being provided?

i. How do U.S. IaaS providers expect to implement this special measure?

Definitions:

[9] *Id.*

12) E.O. 13984 defines "United States person" to mean "any United States 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."[10] It also defines "United States Infrastructure as a Service Provider" to mean "any United States Person that offers any Infrastructure as a Service Product."[11]

a. What should the Department consider when determining whether a foreign subsidiary of a parent U.S. IaaS provider entity would be subject to the regulations implementing E.O. 13984? What implications for international commerce would there be, if any, if foreign subsidiaries were covered by the rule?

Overarching Inquiries:

13) What key differences in industry makeup, market dynamics, and general business practices should be taken into consideration when drafting E.O. 13984's proposed rule language compared with similar regulatory frameworks in other industries (such as the Financial Crimes Enforcement Network's Customer Due Diligence and 311 Special Measure regulations)?

14) Foreign malicious cyber actors often are able to acquire and provide fake names, government documents, and other identification records, making it increasingly difficult for IaaS providers to verify identities in a timely fashion. Do commenters believe that the Department should place more emphasis on ongoing customer-due-diligence efforts instead of initial Account creation requirements? How might this approach better accomplish E.O. 13984's goals to deter foreign malicious

[10] EO 13984 at 6841.
[11] *Id.*

cyber actors' use of United States IaaS products, and to assist in the investigation of transactions involving foreign malicious cyber actors?

15) Are there fraud-prevention regimes—whether regulatory or technical—used in other industries (e.g., finance) that would enable the more consistent discovery of the use of fake names, government documents, and other identification records when establishing Accounts with U.S. IaaS providers?

Dated: September 16, 2021

Trisha B. Anderson,

Deputy Assistant Secretary, Intelligence & Security,

U.S. Department of Commerce.

[FR Doc. 2021-20430 Filed: 9/23/2021 8:45 am; Publication Date: 9/24/2021]