FOR IMMEDIATE RELEASE
January 29, 2024
https://bis.doc.gov

BUREAU OF INDUSTRY AND SECURITY
Office of Congressional and Public Affairs
Media Contact: OCPA@bis.doc.gov

Commerce Proposes Rule to Advance U.S. National Security Interests and Implement Biden-Harris Administration's AI Executive Order and National Cybersecurity Strategy

Proposed Rule Seeks to Improve Detection and Prevention of Foreign Malicious Cyber Activity and Prevent U.S. Services from being Used Against U.S. Interests

WASHINGTON, D.C. – Today, the Department of Commerce (Department) published a notice of proposed rulemaking (NPRM) for establishing new requirements for Infrastructure as a Service providers (IaaS or "cloud infrastructure providers"). The NPRM outlines proposed requirements to address the risk of foreign malicious actors using U.S. cloud services that could be used in malicious cyber-enabled activity to harm U.S. critical infrastructure or national security, including to train large artificial intelligence (AI) models.

This NPRM demonstrates the Biden-Harris Administration's proactive efforts to address the potential national security risks associated with frontier AI models and the abuse of U.S. cloud infrastructure by malicious actors and is a significant step in implementing the President's Executive Order (EO) on "Safe, Secure, and Trustworthy Use and Development of Artificial Intelligence" (EO 14110) and the National Cybersecurity Strategy.

"Today's rule puts foreign malicious cyber actors on notice that we are taking action to prevent them from using our own cloud infrastructure to undermine our national security interests," **said Under Secretary for Industry and Security Alan Estevez**. "Today's proposed rule gives the Secretary of Commerce the tools she needs to address risks while maintaining the Department's overall approach to national security: to innovate and do business wherever we can, and to protect what we must."

The proposed rule introduces potential regulations that require U.S. cloud infrastructure providers and their foreign resellers to implement and maintain Customer Identification Programs (CIPs), which would include the collection of "Know Your Customer" (KYC) information. Similar KYC requirements already exist in other industries and seek to assist service providers in identifying and addressing potential risks posed by providing services to certain customers. Such risks include fraud, theft, facilitation of terrorism, and other activities contrary to U.S. national security interests.

The NPRM also authorizes the imposition of certain special measures that can restrict malicious cyber-enabled actors' access to U.S. IaaS. In this NPRM, the Department seeks feedback on a number of issues, including: minimum verification standards, access, and record-keeping requirements that providers must adopt; the procedures by which the Secretary of Commerce decides when and how to impose a special measure; and the definitions of several key IaaS and AI-related terms as they apply to the regulations.

This NPRM incorporates many of the public comments received in response to a September 24, 2021, Advanced Notice of Proposed Rulemaking (ANPRM). That ANPRM sought feedback on how the Department should implement various provisions of EO 13984, "Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber Enabled Activities." Based on these comments, the Department has drafted the proposed rule to clarify requirements for the public in ways that are consistent with industry and public understanding of IaaS-related products and services.

The text of the proposed rule released today is available on the Federal Register's website here. The deadline for public comments is April 29, 2024.

About the Office of Information and Communications Technology and Services:

The ICTS program became a mission of BIS in 2022. OICTS is charged with implementing a series of Executive Orders (EOs) under the International Emergency Economic Powers Act (IEEPA) focused on protecting domestic information and communications systems from threats posed by foreign adversaries.

The ICTS program's authorities include:

1. EO 13873, "Securing the Information and Communications Technology and Services Supply Chain" (May 15, 2019), delegated to the Secretary of Commerce broad authority to prohibit or impose mitigation measures on any ICTS Transaction subject to United States jurisdiction that poses undue or unacceptable risks to the United States.

2. 15 C.F.R. Part 7, "Securing the Information and Communications Technology and Services Supply Chain," is the implementing regulation for EO 13873 and establishes the scope of an ICTS Transaction and creates a process for reviewing ICTS Transactions the Department or other agencies (through referrals) believe may pose an undue or unacceptable risk. The Department can, on its own accord or upon referral, investigate ICTS Transactions. Ultimately, the Secretary can prohibit or mitigate ICTS Transactions if those transactions pose one of the three risks outlined in EO 13873.

3. EO 13984, "Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities" (January 19, 2021), directs the Secretary of Commerce propose rules to address malicious cyber actors' use of Infrastructure as a Service (IaaS), by proposing "know your customer" (KYC) requirements.

4. EO 14034, "Protecting Americans' Sensitive Data from Foreign Adversaries" (June 11, 2021), builds upon EO 13873 to address threats posed by connected software applications linked to foreign adversaries.

5. EO 14110, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" (October 30, 2023), builds on E.O. 13984, directing the Secretary of Commerce to impose record keeping requirements on IaaS providers when transacting with a foreign person to train certain large AI models.

For more information, visit www.bis.doc.gov.

###