ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

October 25, 2021

Trisha B. Anderson
U.S. Department of Commerce
1401 Constitution Avenue NW
Washington, DC 20230

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

Dear Ms. Anderson,

The Information Technology and Innovation Foundation (ITIF) welcomes the opportunity to submit comments in response to the advance notice of proposed rulemaking (ANPRM) on "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities." ITIF is a non-profit, non-partisan public policy think tank focusing on technological innovation and public policy.

The Commerce Department produced the ANPRM in response to Executive Order 13984, issued January 19, 2021, which directs the Secretary of Commerce to implement regulations to deter foreign malicious actors from using U.S. Infrastructure as a Service (IaaS) cloud services. Particularly problematic are Section 1 of the executive order, which would establish rules for U.S. IaaS providers to verify the identity of foreign customers, and Section 2, which would implement special measures if the U.S. government determines foreign actors are abusing U.S. IaaS services.

While ITIF agrees with the goal of the executive order—to ensure that foreign actors do not exploit U.S. cloud computing resources for malicious cyber activities—the proposed solutions have multiple deficiencies which would not only render them ineffective, but also undermine the competitiveness of U.S. cloud computing providers. At a time when U.S. cloud providers are seeking to compete in foreign markets and the U.S. government is seeking to negotiate a successor to the EU-US Privacy Shield agreement, this proposal could undermine trust in U.S. cloud providers by creating the appearance, if not the reality, of potentially inappropriate interference by the U.S. government of foreign users of domestic IaaS cloud service providers.

IDENTITY VERIFICATION IS COMPLEX AND CREATES NEW RISKS

Section 1 of the executive order proposes that U.S. IaaS providers verify the identity of foreign account holders either upon opening an account or during maintenance of an existing account. The goal of having service providers collect more information about their business customers is to stop bad actors from using legitimate services to engage in illegal activity. This concept originated in anti-money laundering laws which require banks and other financial institutions to verify the identity of their customers (both consumers and businesses). The European Union may also include a "know your business customer" (KYBC) obligation in the Digital Services Act, pending legislation that would apply to online intermediaries. The KYBC requirement would only apply to business-to-business relationships, so they would exclude consumers. There is some merit to the idea of service providers collecting more information about their business customers as this could make it possible to take legal action against lawbreakers, including spammers, counterfeiters, and distributors of malware and digital piracy, but the current challenges make any requirement to do so unreasonable.

First, while the executive order suggests the identity verification requirements would only apply to foreign customers, cloud service providers cannot easily distinguish between domestic and foreign customers. Indeed, there is no way to effectively distinguish between foreign and domestic customers without requiring domestic customers to also prove their identity to show that they are not a foreign customer (otherwise it would be trivial for a foreign customer to avoid these requirements by asserting that they are a domestic customer).

Second, verifying identities is not a trivial exercise. In the absence of widely available electronic identification (eIDs), identity verification is a manual process. As a result, cloud service providers would be tasked with manually verifying identity documents or proof of business registration in multiple languages from countries around the world—all remotely. Most cloud service providers are not equipped to handle this task or complete it effectively to prevent fraud. Therefore, imposing this type of requirement could add substantial delays to onboarding new customers which could make U.S. cloud service providers less attractive to foreign customers.

Third, sharing all of these identity documents would create new data privacy risks for customers of U.S. cloud providers, as they would be required to provide sensitive personal and business information in an unsecured format (e.g., scans of paper identity documents). Law-abiding foreign customers might simply opt to go with an alternative non-U.S. cloud provider to avoid this risk. In addition, hackers may specifically target U.S. IaaS cloud service providers in order to illegally obtain these identity proofing documents.

Finally, and perhaps most importantly, it is important to understand that the intended goal of these provisions is to identify and stop unlawful foreign customers, and these bad actors are not going to play by the rules. They will lie and cheat to gain access to U.S. IaaS services, such as by using stolen payment credentials, masquerading their identity, hiding behind a network of shell companies, or buying access to verified IaaS accounts in the underground economy. Therefore, any identity verification requirements should be designed

with the assumption that those bad actors the government most wants to find will be the ones most likely to attempt to circumvent and adapt to the requirements.

CREATING BROAD "SPECIAL MEASURES" WOULD UNDERMINE U.S. CLOUD COMPETITIVENESS

Section 2 of the executive order specifies that the U.S. government can impose "special measures" that U.S. IaaS providers will be required to take including, 1) prohibitions or conditions on opening or maintaining an account by any person located in a designated foreign jurisdiction; and 2) prohibitions or conditions on opening or maintaining an account by certain foreign persons. While these special measures can only apply when the U.S. government deems that either a foreign jurisdiction has a "significant number of foreign persons directly obtaining United States IaaS products for use in malicious cyber-enabled activities" or a foreign person "has established a pattern of conduct of offering…or directly obtaining United States IaaS products for use in malicious cyber-enabled activities," the order creates a broad authority for the U.S. government to intervene in the accounts of foreign IaaS customers.

Such a broad, and potentially intrusive, authority will make it harder for U.S. cloud service providers to compete in foreign markets. Foreign customers often express reservations about potential U.S. government access to their systems and data, and this new authority would only exacerbate their concerns. In particular, given the sensitive dialogues between the United States and the European Union over implementing a successor to the EU-US Privacy Shield, pursuing this new authority now would be untimely and counterproductive. The Secretary appears to have the authority to indefinitely delay enacting these special measures as the executive order notes that in considering these special measures the Secretary should consider "significant adverse effect on legitimate business activities" as well as "the effect of any special measure on United States national security, law enforcement investigations, or foreign policy."

Moreover, these broad special measures are likely unnecessary. The U.S. government already has authority to restrict exports of cloud services to certain foreign countries or designated foreign businesses through the Department of Commerce's Bureau of Industry and Security's Entity List and other export controls.

A PATH FORWARD

There are fundamental flaws with Sections 1 and 2 of the executive order, and ideally, the Biden administration will rescind this directive so as not to put the U.S. cloud computing industry at a competitive disadvantage. Moreover, ideally any requirements would be compatible with the EU's Digital Services Act to reduce the compliance burden, so rather than rushing through any new regulations, it should be coordinated with the EU, such as through the US-EU Trade and Technology Council.

However, there are opportunities for addressing this issue. Section 3 directs the Commerce Secretary, in coordination with the Attorney General and the Secretary of Homeland Security, to coordinate and solicit feedback on voluntary information sharing and collaboration with industry to address these concerns. This path offers the most promise for improving the ability of U.S. IaaS cloud service providers to address the risk of foreign actors using their services to engage in malicious cyber activities. For example, the public and

private sector may work together to identify best practices for detecting malicious activity on IaaS accounts, coordinate efforts to identify and stop unscrupulous resellers of IaaS services, share information to investigate and prosecute those using IaaS services to engage in illegal activities, and create an industry roadmap for verifying the identity of cloud customers. They may also be able to research the effectiveness of proposed regulatory solutions so that the Department of Commerce has more evidence on which to base future proposals.

Sincerely,

Daniel Castro
Vice President, Information Technology and Innovation Foundation