October 25, 2021

Trisha B. Anderson
Deputy Assistant Secretary for Intelligence and Security
US Department of Commerce
1401 Constitution Avenue NW
Washington, DC 20230

Via email to IaaScomments@doc.gov

Dear Ms. Anderson:

BSA | The Software Alliance[1] appreciates the opportunity to provide the below comments on the US Department of Commerce's Advanced Notice of Proposed Rulemaking (ANPRM) implementing Executive Order 13984 (EO), on Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities, signed by President Trump on January 19, 2021.

BSA is the leading advocate for the global enterprise software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, providing the products and services that power other businesses. BSA members are also leaders in security, having pioneered many of the software security best practices used throughout the industry today.

BSA supports the goal of Executive Order 13984 to deter the use of United States IaaS products by foreign actors for malicious cyber-enable activities. The US Government, and governments around the world, should partner with cloud providers to promote practices to

[1] *BSA's members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, CNC/Mastercam, DocuSign, IBM, Informatica, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.*

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

reduce IaaS product abuse by malicious actors. Further, BSA appreciates the Department of Commerce's decision to proceed using an ANPRM rather than another regulatory vehicle.

The Executive Order directs the Secretary to propose regulations that (I) require US infrastructure as a service (IaaS) providers to verify the identity of a foreign person who obtains an account and permits the Secretary to exempt an IaaS provider from the requirements of this regulation; and (II) implement special measures to prohibit or impose conditions on accounts within certain foreign jurisdictions or of certain foreign persons. While BSA supports the overall objective of the EO, requiring additional collection and retention of customer information and granting the Secretary wide discretion to prohibit or restrict certain transactions will have negative consequences on US IaaS providers and will not meaningfully address the objectives of the EO.

First, most US IaaS providers take the defense of their services seriously and invest considerable resources to prevent, detect, and mitigate abuse for both business and security purposes. They create and run programs to identify and stop malicious activity, share cyber threat information with relevant stakeholders, and alert law enforcement where criminal referral is appropriate. However, the diversity of the people, processes, and techniques IaaS providers use to prevent, detect, and mitigate abuse underscores the need for IaaS providers to be agile in their response to dynamic threat actors and reflects the fact that there are multiple ways to accomplish that important goal. Consequently, any regulations proposed under the EO should ensure IaaS providers have the flexibility to continue diverse and innovative ways to reduce abuse. Notably, the EO allows the Secretary to exempt IaaS providers that meet certain security best practices. BSA recommends that such exemption apply to those IaaS providers that have a due diligence program for screening customers and addressing use of their services for malicious cyber purposes.

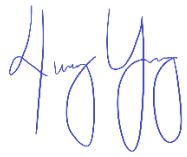
Second, while BSA accepts that laws and policies need not be perfect to be helpful, it is unlikely that the regulations envisioned in President Trump's Executive Order will produce benefits that outweigh their costs. Malicious actors who are sophisticated enough to launch cyber attacks from US IaaS providers—many of whom are supported by foreign governments—are also sophisticated enough to evade the data collection and retention requirements envision by this EO. As the ANPRM notes, "Foreign malicious cyber actors often are able to acquire and provide fake names, government documents, and other identification records." As a result, regulations requiring the collection and retention of such information are likely to increase the burden on US IaaS providers, which will result in these companies being less competitive, while not addressing the malicious activity noted in the ANPRM.

Third, the Department of Commerce should consider the substantial likelihood that the US Government imposing a regulatory requirement to collect and retain customer information will justify similar requirements by other governments.

Fourth, the Secretary of Commerce's willingness to impose conditions on accounts of foreign persons will create uncertainty and introduce untenable risk for US companies seeking to compete globally. Customers will be reticent to contract with US IaaS providers knowing that the infrastructure on which they rely to operate is subject to the special measures contained in Section 2(d) of the EO, which provides the Secretary the authority "prohibit or impose conditions on the opening or maintaining . . . an account" within certain foreign jurisdiction or with certain foreign persons, with extremely limited procedural protections. It is difficult to imagine how the Secretary of Commerce could retain the near limitless discretion to prohibit accounts with foreign jurisdiction or persons yet mitigate any competitive disadvantage created by the uncertainty.

Thank you for considering BSA's views. We look forward to continuing to work with the US Department of Commerce on this important effort.

Sincerely,



Henry Young
Director, Policy