IST Institute for SECURITY + TECHNOLOGY

IST Leadership

Mike McNerney
Chair, Board of Directors

Philip Reiner
Chief Executive Officer

Megan Stifel
Chief Strategy Officer

Steve Kelly
Chief Trust Officer

Institute for Security and Technology
195 41st Street #11045
Oakland, CA 94611

April 29, 2024

Under Secretary Alan Estevez
Bureau of Industry and Security
U.S. Department of Commerce
1401 Constitution Ave NW
Washington, DC 20230

Subject: Comments on the Notice of Proposed Rulemaking on *Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities*; 88 Fed. Reg. 5698, RIN 0694-AJ35, Docket No. 240119-0020; DOC-2021-0007.

Dear Under Secretary Estevez,

The Institute for Security and Technology (IST) appreciates the opportunity to file comments in response to the Bureau of Industry and Security's (BIS's) Notice of Proposed Rulemaking on *Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities*, issued pursuant to Executive Orders 13984 and 14110.

As a 501(c)(3) think tank focused on emerging security problems, including cybersecurity and Artificial Intelligence, we launched a study to develop options for establishing Abuse of IaaS Products Deterrence Programs (ADPs) under § 7.306 of the proposed rule–to include a "consortium" approach–through which providers might be exempted from the rule's Customer Identification Program (CIP) requirement. As is typical of IST's studies, we convened a number of industry stakeholders to gather input and consulted those experienced with "know your customer" practices within the financial services sector. We are also considering the findings and recommendations of the National Security Telecommunications Advisory Committee's report to the President on *Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors*. While our work remains ongoing, we would like to share some initial observations.

Customer identification requirements may ultimately prove to be of limited value in deterring abuse of IaaS products, but at the same time carry distinct downsides. Among these include the negative optics for U.S. providers in

the global marketplace by requiring they treat U.S. and foreign customers differently. This requirement may lead bad actors to increase the use of U.S. Person (USPER) strawman subscribers, or simply use fake USPER personas buttressed by a U.S. Internet Protocol address at the time of enrollment. Either of these might allow the actor to evade increased scrutiny under the rule and potentially create a false sense of security. Furthermore, such requirements would likely present a mere inconvenience to sophisticated state actors.

On the other hand, we see potential for the rule's ADP alternative—particularly if providers are joined through a consortium as suggested in § 7.306(c)—making the ecosystem less hospitable to malicious cyber actors over the long term. One might even imagine a scenario in which a consortium provides sufficient value that foreign IaaS providers operating in like-minded states (e.g., "Five Eyes" nations and the European Union) might voluntarily join, thus increasing the ecosystem-level benefit.

While BIS's rulemaking is undoubtedly constrained by E.O. 13984's inherent structure and logic, the comparative advantages of the ADP vs. CIP approaches lead IST to recommend that the presumption be flipped. However, making the ADP path viable would nonetheless require the following adjustments:

- **Allow time for good-faith efforts to establish an ADP.** Establishing an ADP, particularly one that includes a consortium approach, will require time, effort, and resources. Since it is our view that an ADP will have significantly greater potential to achieve E.O. 13984's stated purpose over establishing a CIP (while also eliminating the downsides described above) we encourage BIS to consider adding a provision that stops the CIP requirement clock while this process plays out. If the good-faith effort is not successful, or deemed insufficient by your agency, then the one-year CIP requirement clock can begin counting down at that point.

- **Specify minimum elements of an ADP.** Uncertainty drives risk, and thus, lack of confidence that an ADP application will succeed may lead some IaaS providers to simply establish a CIP. Providers will be much more amenable to pursuing the ADP route if the rule were to provide guidance describing minimum elements or best practices (i.e., a standard) upon which BIS would evaluate such applications. This will also serve our next observation. IST's study process is gathering our recommended list of best practices, which we will publicly report in the coming months. We also recommend BIS

engage stakeholders directly for feedback on this question, and consider that such best practices will likely need to evolve over time.

- **Provide due process for ADP revocation.** Since the rule by default requires providers to establish a CIP, it follows that providers may be hesitant to pursue the more beneficial ADP route if they lack assurances that a successful application will remain acceptable over time. Were BIS to judge a provider's previously approved ADP as no longer sufficient and therefore revoked, the provider would find themselves suddenly non-compliant for lack of a CIP. Therefore, to ensure trust and confidence in the ADP route, BIS might consider including due process provisions in the event that an ADP is found lacking, including a reasonable opportunity to remedy shortcomings.

IST looks forward to an opportunity to consult with your staff, and that of other relevant U.S. departments and agencies, as we progress in our study effort. Thank you for considering our comments.

Regards,

Steve Kelly
Chief Trust Officer