April 29, 2024

The Honorable Gina Raimondo
Secretary
U.S. Department of Commerce
1401 Constitution Ave NW
Washington, DC 20230

RE: E.O. 13984/E.O. 14110 NPRM; DOC-2021-0007

Dear Secretary Raimondo:

The undersigned associations respectfully submit this letter on behalf of our member companies regarding the Notice of Proposed Rulemaking (NPRM) issued on January 29, 2024 to implement *Executive Order on Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities* (referred to hereafter as the "Infrastructure as a Service" (IaaS) EO), as well as the *Executive Order on Safe, Secure, and Trustworthy AI* (hereafter the "AI EO").

Our members have and will continue to partner with the U.S. Government (USG) to address cyber and national security threats, including the potential risks associated with the training of large AI models with potential capabilities that could be used in malicious cyber-enabled activity. Our members take seriously their responsibility to protect against malicious actors using their services to perpetrate crimes. While we understand Commerce was tasked with developing implementing regulations for these Executive Orders, we believe that the Customer Identification Program (CIP) will do little to address the national security concerns articulated in the EOs and will instead detract from efforts that will actually address the issues the government is seeking to address. We are likewise concerned that the reporting requirements for large AI models will undermine trust in U.S. IaaS providers.

**We respectfully ask that the USG reconsider the proposed approach to the Customer Identification Program (CIP), taking into account the findings and recommendations included in the National Security Telecommunications Advisory Committee report on *Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors*.**[1] We recommend that the U.S. government place greater emphasis on the Abuse of IaaS Products Deterrence Program (ADP), proposed in 7.306(b) and related exemptions instead of the CIP. We believe that the ADP exemption, if further strengthened, will incentivize providers across the ecosystem to adopt cybersecurity best practices, which will in turn

[1] National Security Telecommunications Advisory Committee report available here: https://www.cisa.gov/sites/default/files/2024-01/NSTAC_Report_to_the_President_on_Addressing_the_Abuse_of_Domestic_Infrastructure_by_Foreign_Malicious_Actors_508c.pdf

more effectively address abuse of IaaS services. One way for the Commerce Department to strengthen the ADP exemption would be to prioritize collaboration with industry to identify and develop additional best practices to deter malicious abuse of cloud infrastructure. We highlight that our member companies are in many instances, already implementing best practices aimed at deterring abuse of their IaaS offerings, including instituting account creation requirements, undertaking behavior-based risk analysis, building-in protections for malicious behavior, proactively implementing processes to detect and stop suspicious behavior, and undertaking expeditious incident response.

We understand that the intent of the rulemaking and underlying IaaS EO is to deter bad actors, but we believe that the CIP is unlikely to achieve this objective and will instead undermine trust in U.S. IaaS providers and negatively impact U.S. technological leadership and competitiveness. The emphasis on the creation of a CIP will not adequately address abuse of critical cyber infrastructure by malicious actors. On the contrary, threat actors that leverage IaaS or other IT resources to conduct malicious activities are unlikely to provide legitimate identifying information and will not be deterred by a requirement to produce such information. The NSTAC study concluded that such verification requirements are unlikely to decrease the abuse of domestic infrastructure by malicious foreign actors.[2] The NSTAC recommended establishment of an Abuse Deterrence Program as a better option, which we support as a more targeted and effective mechanism for achieving the aims set forth in Executive Order 13984.

Further, requiring IaaS providers to collect and retain personal information as a part of a CIP will have significant privacy implications, especially in the European Union but also in other countries around the world. International customers may worry that that U.S. IaaS providers are being directed to collect and retain Personally Identifiable Information for the purpose of sharing with law enforcement, undermining trust in U.S. IaaS providers. This could serve to heighten tensions regarding data privacy issues and international data transfers, specifically when it comes to the adequacy decision of the EU Commission related to the EU-U.S. Data Privacy Framework. It may also disincentivize customers from using U.S. services, jeopardizing legitimate business, and undermining U.S. competitiveness.

**We also ask that the Commerce Department split the rule in two so that the AI model reporting requirements can be considered separately.** Such an approach would allow Commerce more time to collaborate with stakeholders and rework the AI model reporting requirements to account for legal, technical, and policy shortcomings that undermine the effectiveness of the rule as currently constructed and make it harder to realize the potential benefits of a more narrowly targeted approach. For example, the USG should clarify if and how the rule interacts with the Stored Communications Act, which prohibits remote computing services from disclosing customer records absent legal process. The USG should also consider that the current structure of the rule is not practically implementable,

[2] Ibid.

given the fact that IaaS providers do not readily have access to the information on their customers, such as AI training practices or cybersecurity practices, which they would be required to collect and report. Additionally, Commerce should consider scoping the large AI model reporting requirement to countries of concern, to avoid undermining relationships with allies and partners that rely on the safe, secure, and trustworthy cloud services offered by U.S. IaaS providers.

We appreciate the opportunity to share our perspectives and reiterate our commitment to working with the U.S. government to further our national security goals.

Sincerely,

Alliance for Digital Innovation
Computer & Communications Industry Association (CCIA)
Cyber Threat Alliance
Cybersecurity Coalition
Information Technology Industry Council (ITI)
Internet Infrastructure Coalition
Japan Electronics and Information Technology Industries Association (JEITA)
National Foreign Trade Council (NFTC)
Representative of German Industry and Trade (RGIT)
Software & Information Industry Association (SIIA)
U.S. Chamber of Commerce

CC:
The Honorable Anne Neuberger, Deputy Assistant to the President and National Security Advisor for Cyber and Emerging Technologies, White House
The Honorable Harry Coker, National Cyber Director, White House
The Honorable Alan Estevez, Under Secretary for Industry and Security, U.S. Department of Commerce
Elizabeth Cannon, Executive Director, Office of Information and Communications Technology and Services, Bureau of Industry and Security, U.S. Department of Commerce