U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

October 25, 2021

Ms. Trisha B. Anderson
Deputy Assistant Secretary
Intelligence & Security
U.S. Department of Commerce

Re: EO 13984, Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities

Dear Ms. Anderson:

The U.S. Chamber of Commerce (the Chamber) appreciates the opportunity to provide the Department of Commerce (the Department) feedback on the Trump Administration's Executive Order 13984 (EO 13984) *Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities*.

Our members remain committed to supporting and enhancing the national security of the U.S., which includes strengthening resilience to cyber threats posed by hostile foreign adversaries and advanced persistent threat actors. Businesses confront advanced, persistent, often state-sponsored, cyberattacks that are increasingly sophisticated. Cyberspace remains the only domain where private companies must defend themselves against nation states or their proxies. These challenges are real, and their complexity deserves thoughtful responses that blend a mix of new cybersecurity requirements with incentives to U.S. infrastructure-as-a-service (IaaS) providers. Such an approach would increase security and resilience controls commensurate with the risk and threat.

As we noted in our January 27th letter to Acting Office of Management of Budget Director Robert Fairweather, the Chamber supports the goal of EO 13984. We urge the Department, however, to consider our serious concerns as it examines next steps. Specifically, we are concerned that EO 13984:

1. Overlaps with Executive Order 14028.
2. Falls short of its policy objectives;
3. Misaligned with existing layers of cyber defenses;
4. Undermines U.S. IaaS providers ability to compete globally, specifically in the European Union; and
5. Disrupts ongoing data flows negotiations with the European Union.

Overlaps with Executive Order 14028 : As the Department considers next steps, we urge it to consider aligning with and supporting existing mechanisms to address the concerns highlighted in EO 13984. As President Biden noted earlier this year in Executive Order 14028 (EO 14028), *Improving the Nation's Cybersecurity*, the U.S. faces persistent and increasingly sophisticated adversarial campaigns that threaten the security and privacy of public and private entities. While EO 14028 focuses on improving the federal government's security posture, it also underscores the importance of collaborating with the private sector. We see two areas of potential overlap and duplication that are cause for concern.

First, Section 2 of EO 14028 directs federal agencies to review and remove barriers to sharing threat information across government and between the government and the private sector. This appears to be a substantially similar line of effort with Section 3 of EO 13984 that tasks the Department of Homeland Security to engage and solicit feedback from industry on how to increase information sharing and collaboration among IaaS providers and between IaaS providers and the agencies.

Second, Section 3 of EO 14028 outlines several policy and security objectives related to cloud services including (1) a requirement for federal agencies to prioritize resources for the adoption and use of secure cloud technologies, (2) the development of a federal cloud-security strategy, (3) the development and issuance of a cloud-security technical reference architecture, and (4) the development and issuance of a cloud-service governance framework.

We believe these potentially overlapping and duplicative processes complicate the ability of U.S. businesses to partner with U.S. government and undermine the capability to enhance the resilience of U.S. IaaS providers. The Chamber encourages the Biden Administration to take a whole-of-government approach, integrating existing efforts, scoping current workflows, and coordinating towards a unity of effort to increase public-private operational collaboration in cyber defense. An example of this approach can be found in the Cybersecurity and Infrastructure Security Agency's (CISA) Joint Cyber Defense Collaborative (JCDC) initial sprint on preventing adversarial attacks on cloud services through the execution of cyber defense operations plans. CISA's whole-of-government led efforts, paired with a more strategic approach to cloud resilience, could promote effective IaaS provider practices for reducing abuse.

Falls short of policy objectives: Section 1 of Executive Order 13984 requires U.S. cloud service providers to collect certain information from its customers, including national identification information, email, phone, internet protocol (IP) address, and payment information. Working to address adversarial abuse of cloud services is important, but the Chamber is concerned that Section 1 will have limited positive impact reducing cyber risk while resulting in high privacy and trust costs. Within the privacy context, we are concerned with the requirement to collect and retain national identification information, especially given challenges with global systems to verify such information in a digital environment and the likelihood that threat actors may use falsified information to obfuscate their unlawful activity. The provision will have a significant impact on the digital economy and the global competitiveness of U.S. IaaS providers without achieving the desired security outcomes.

Misaligned with Existing Layers of Cyber Defenses: Many U.S. IaaS providers already invest significantly in security and fraud prevention programs to counter nefarious activity. Requiring additional data collection and retention will not provide the additional security the EO aims to achieve. It may be reasonably assumed that illicit actors falsify or conceal their identities to IaaS providers when establishing new accounts. U.S. IaaS providers regularly disrupt malicious activity and reduce abuse of IaaS products by continuously monitoring for anomalous behavior; detecting abuse; and removing illicit accounts, when appropriate (e.g., through subscription takedowns). Nevertheless, more work needs to be done on establishing industry consensus on best practices for reducing, detecting, and responding to cloud abuse. There is a genuine willingness on the part of U.S. IaaS providers to promote superior risk management controls, processes, and procedures.

Undermines U.S. IaaS providers' ability to compete globally, specifically in the EU: The Chamber is a longtime advocate for strong commercial ties between the U.S. and the European Union and is a leading business voice on digital economic policy.[1] In the U.S., Europe, and globally, we advocate for sound policy frameworks that support economic growth, promote data protection, and foster innovation. Many of the Chamber's members are heavily invested in the EU, which is collectively the largest primary U.S. export market. The Chamber is concerned that the implementation of EO 13984 will jeopardize U.S. IaaS providers global competitiveness, especially in the European cloud marketplace. From the outset the Chamber has conveyed that this EO will negatively affect the ability of U.S. IaaS providers' to compete in the EU at a time that when European member states are actively supporting policies and programs that are likely to exclude U.S. cloud service providers from the digital single market (e.g., GAIA X initiative, French SecNumCloud, EU cloud security scheme, the future Cloud Rulebook). This EO could further undermine U.S. competitiveness in the EU marketplace.

Disrupts ongoing data flows negotiations with the EU: The Chamber shares the U.S. government's concern regarding the implications of the Schrems II decision for companies' continued ability to transfer data across the Atlantic. As we have outlined to leaders in Washington and Brussels, a key priority of governments on both sides of the Atlantic, together with the business community, must be to restore legal certainty to data flows between the U.S. and EU. However, the data collection and retention requirements in EO 13984 could raise concerns anew. We note with interest the statement and following program of work by the OECD Committee on Digital Economy Policy, which confirms that data flows are integral to the global digital economy and a necessary input for reaping the benefits of digitalization. As fellow democracies and strategic allies that value consumer privacy, and share a common national security interest, the U.S. government and European Commission must agree quickly on a new agreement on data flows.

The Chamber values its collaborative relationship with the Department on a range of cybersecurity initiatives. The *Cybersecurity Framework* and the core security baseline for IoT devices, both led by the National Institute of Standards and Technology (NIST), represent some of the best examples of public-private partnerships in action. In addition, the Chamber values the engagement from the National Telecommunications and Information Administration (NTIA) on efforts to implement the National Strategy to Secure 5G and supports the open and constructive efforts for a Software Bill of Materials.

---

[1] The Chamber is also committed to being proactively engaged in the work of the new U.S.-EU Trade and Technology Council. Our initial policy priorities for this new platform are available here.

The Chamber looks forward to sustained engagement and discussion with the Biden Administration on the underlying cyber threat, approaches to address the threat holistically, current mitigation measures employed by cloud service providers, and opportunities for ensuring American competitiveness in the global marketplace. We also trust that any future actions in this area will respect domestic privacy laws and regulations and support longstanding U.S. priorities to enable the flow of personal information across international borders, including ongoing efforts to negotiate an enhanced data transfer framework with the European Union (EU).

For these reasons, we believe a more sensible approach would be to rescind EO 13984 and focus instead on public and private efforts to enhance the resilience of U.S. IaaS products. We recommend that the USG leverage the framework of President Biden's EO 14028 or look to existing mechanisms that foster collaboration between the public and private sectors. Rescinding the EO in question would enable more effective focus on security and resilience measures that are better calibrated to address the concerns raised in EO 13984, strengthen cyber defenses, raise the costs on malicious cyber actors, and reduce the risk of future significant malicious cyber-enabled activities in a manner that minimizes costs to Americans.

We look forward to engaging with your Department and the broader Administration to strengthen our collective defense in practical ways and help counter adversarial use of cloud infrastructure in a more risk-based manner.

Sincerely,

Christopher D. Roberti
Senior Vice President,
Cyber, Intelligence, and Supply Chain Policy
U.S. Chamber of Commerce

Vincent M. Voci
Vice President,
Cyber Policy
U.S. Chamber of Commerce