THE US-CHINA BUSINESS COUNCIL
美 中 贸 易 全 国 委 员 会

USCBC Comment on Bureau of Industry and Security; Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities.

Department of Commerce, Bureau of Industry and Security, Docket No. 240119-0020

The US-China Business Council (USCBC) welcomes the opportunity to submit comments to the Department of Commerce on its proposed rule "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities," which implements EO 13984 and EO 14110.

USCBC represents over 270 American companies that do business in China, including IaaS providers, as well as many companies that use cloud applications to manage their global operations. Our membership includes some of the largest and most iconic American brands, in addition to small- and medium-sized enterprises.

We support the Biden administration's whole-of-government approach to protect America against malicious cyber activities. Our businesses are stronger, whether it be in the United States or abroad, when networks are secure. USCBC strives to act as a constructive partner to the Biden administration in thwarting bad actors and protecting US critical infrastructure and information.

USCBC also supports the need to continue the United States' long-standing support for free and open cross-border data flows. The free-flow of data and the provision of cross-border services are foundational elements of digital trade that benefit US companies and the economy. We are concerned that certain elements of the proposed rule, or the implementation thereof, may contradict these guiding principles.

We are similarly concerned that the proposed rule, as written, could result in data localization practices that benefit US companies' international competitors. Data innovation and the services that undergird it are essential to US companies' international competitiveness, and the government should endeavor to encourage, not stymie, these newfound drivers of global growth and success. Requiring companies to collect the data outlined in the rule could place US companies at odds with longstanding contractual obligations, local data privacy regulations, and other laws that would prohibit the facilitation of data collection and sharing with third parties such as the US government.

USCBC is concerned that the proposed rule's provisions on IaaS are overly broad, lack needed clarity, and, if implemented as written, risk inadvertent harm to the international competitiveness of cloud service providers. Further, USCBC is concerned that the proposed regulations are not properly calibrated to prevent or deter malicious cyber actors. Malicious actors are entirely capable of providing valid company, identification, or end use information unlikely to flag or prevent misuse of IaaS products. The Bureau of Industry and Security (BIS) should work with industry to set out a system that is narrowly targeted to address national security objectives without undermining US competitiveness globally.

Combating attacks from adversaries, including those perpetrated using domestic infrastructure, requires continuous and iterative international cooperation and an understanding of the constraints of myriad existing legal frameworks. In our comments below, USCBC strives to act as a resource to BIS and the broader US government. Our submission provides specific feedback on key concepts in the proposed rule and raises wider policy concerns.

I. Definitional Concerns

Reporting requirements for AI models in 7.308 do not conform to current industry practices

USCBC is concerned that AI reporting requirements will result in significant disruptions to business processes due to a mismatch between expectations around the reporting process and what is presently feasible for industry. For example, the AI reporting requirements' provision 7.308(i) states that providers must know whether a transaction could result in the training of a large AI model with potential capabilities that could be used in malicious cyber-enabled activity. Providers are also required to assess the beneficial owner of accounts and must know if AI models on their platforms are "dual use foundation models."

These requirements are problematic for several reasons. Service providers generally do not have visibility into their customers' workloads for privacy and security reasons. Customers store extremely sensitive data on providers' services, which they would not be willing to do if providers could view or access their workloads. Because of this, providers generally do not have access to their customers' models and cannot evaluate their capabilities or training practices. It is extremely unlikely customers would be willing to give this information to providers for reporting to the US government because the information is confidential and proprietary.

Moreover, both domestically and internationally, providers are legally and contractually obligated to moderate their collection, retention, and disclosure of personal identification information that would be otherwise needed to fulfill the AI reporting requirement. In particular, the Stored Communications Act prohibits remote computing services, which would include US IaaS providers, from disclosing customer records without legal process, apart from certain exceptions not relevant here. These are practical legal, contractual, and operational hurdles that US companies are unlikely to overcome. It is essential that BIS adjust its proposed rule so that companies are not placed in contravention with extant domestic and international legal commitments and so that any final rule conforms to present industry practices.

Customer verification requirements are easily circumventable

Customer verification requirements in the CIP requirement, including those which require service providers to identify foreign persons and those requiring the identification of the beneficial owner of customers, are easily circumventable by sophisticated actors. It is especially difficult for the private sector to have at-scale insight into actor identities in the context of routine and highly automated online business transactions. The type of actors that BIS is concerned about, such as state supported and advanced persistent threat (APT) actors, are also the most likely to successfully alter their identity to appear as US persons or use other methods to compromise infrastructure. Creating a program that adequately addresses the threat posed by APT actors should focus on close consultation with industry and within the interagency process. Those consultations should identify and implement effective cybersecurity practices and certification programs without resorting to broad, easily circumventable measures, rather than imposition of a CIP requirement.

ADP program clarification

As currently written, the proposed rule does not offer sufficient differentiation between the Abuse of IaaS Products Deterrence Program (ADP) and the CIP program. While the NPRM lays out steps for requesting ADP exemptions from implementing a CIP, it is not clear that when regulations are implemented, if companies can begin with ADP rather beginning with CIP and requesting an ADP-based exemption later.

Moreover, the vague and discretionary nature of the exemption and the Department of Commerce's ability to revoke an exemption at any time, give providers little incentive to pursue an ADP and implement effective abuse prevention mechanisms. Rather than impose a CIP requirement with ADP as part of a voluntary exemption, BIS should work with industry to develop effective abuse prevention best practices that could form the basis of an ADP. We advise that any future procedures should not take effect without a notice and comment period and a delayed implementation period for companies to bring themselves into compliance.

Applicability to other service products

Given the expansive definition of "IaaS Products" the proposed rule will also disadvantage platform-as-a-service (PaaS), network-as-a-service (NaaS), and software-as-a-service (SaaS) offerings which are arguably captured by the proposed rule. PaaS, NaaS, and SaaS offerings are predefined, i.e., a user of a PaaS, NaaS, or SaaS offering uses the platform or software provided by the PaaS, NaaS, or SaaS provider. The risk of malicious use of PaaS, NaaS, and SaaS offerings are low, and the benefits of reports from PaaS, NaaS, and SaaS providers would be of limited value. Importantly, subjecting SaaS, NaaS, and PaaS providers to these requirements would competitively disadvantage U.S. providers, allowing their European and Asian competitors a clear advantage in engaging current and would-be customers.

II. Implications for Competitiveness

If implemented as written, the proposed rule will place US IaaS providers at an international disadvantage compared to foreign firms that are not encumbered by similar restrictions. Regulations which raise the cost and complexity for US firms paradoxically advantage their Chinese peers such as Huawei and Alibaba, which are the largest IaaS providers after US firms. This trend will be especially prevalent in emerging markets where concerns about foreign data collection are a smaller priority. There, US companies are already engaged in fierce competition with Chinese firms who are bolstered by a sophisticated set of export-oriented industrial policies. State-owned Chinese cloud service companies are also becoming more present in global markets.

Novel controls on IaaS providers and privacy concerns about new data collection requirements for foreign customers may enliven foreign governments' rulemaking processes on digital sovereignty and cyber resilience. This is already happening. For example, Mexico's Fintech Law states that, as part of their business continuity plans, electronic payment funds institutions (IFPEs) must retain access to CSPs from more than one legal jurisdiction. Further, China has strict data privacy regulations and market access requirements for telecom services, which have negatively impacted China's attractiveness as an investment target – the US should not seek to replicate these systems. These regulatory trends, and the proposed rule's impacts on privacy, will disadvantage US firms in global markets. BIS should take foreign regulations and privacy concerns into account when contemplating its next steps, as US-service providers will likely suffer adverse reactions from foreign governments and companies concerned about increased US government oversight in their cloud and AI development ecosystems.

USCBC appreciates the opportunity to comment on the proposed rule and hopes to continue to work with the administration to develop policies that are effective, multilateral, and narrowly tailored, while also promoting US companies' ability to provide secure, reliable services around the world. Doing so is essential to maintaining America's global competitiveness. We also hope to help BIS craft a strategy that balances the administration's security priorities with technological realities and efficiencies inherent to the global cloud ecosystem.