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

USCBC Comment on National Security Division; Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern

Department of Justice, National Security Division, Docket No. NSD 104

The US-China Business Council (USCBC) welcomes the opportunity to submit comments to the National Security Division of the Department of Justice (DOJ) regarding the advance notice of proposed rulemaking (ANPRM) outlining the proposed implementation of the regulations contemplated by the Executive Order (EO) of February 28, 2024, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern."

USCBC represents more than 270 American companies that do business with China. Our membership includes some of the largest and most iconic American brands, in addition to small- and medium-sized enterprises. Our members represent a wide range of industries and sectors, including manufacturers, professional services firms, life-science entities, high-tech companies, financial services firms, and others.

We support the Biden administration's whole-of-government approach to protect Americans' personal and sensitive data. Our businesses are stronger, whether it be in the United States or abroad, when sensitive networks are secure and free from malicious cyber-enabled activities. USCBC strives to act as a constructive partner to the Biden administration in thwarting bad actors engaged in espionage and threatening American citizens and entities.

USCBC also supports the need to continue the United States' long-standing support for free and open cross-border data flows. This is a foundational element of digital trade and data governance that allows US entities to engage in investment and international commerce to the benefit of the US economy. While the EO states that this rule does not diverge from such policy, USCBC remains concerned that segments of the rule, or the implementation thereof, may indeed conflict with that guiding principle. In that same vein, USCBC is similarly concerned that the rule, as written, could potentially result in data localization. Data innovation is a key component of US companies' international competitiveness, and the government should endeavor to encourage, not stymie, data flows that enable newfound drivers of global growth and success.

The United States should not aim to replicate China's system which identifies specific classes of data with corresponding thresholds that require government approval to export. USCBC has consistently advocated to liberalize China's system. The United States government should recall the principles of what has historically fueled America's competitiveness on the world stage, while also securing US national security interests. This means addressing risks in a way that does not create unintended consequences or outcomes that inadvertently further increase such security risks.

In our comments below, USCBC strives to act as a resource to the Department of Justice and the broader US government. Our submission provides specific feedback on key definitions, concepts, and elements posed in the ANPRM.

Executive Summary

To improve compliance with the final rule and any other future regulations under the bulk data ANPRM and to seek to address necessary questions and clarifications with DOJ, USCBC makes the following recommendations:

- Regarding prohibited and restricted transactions, DOJ should not include data that is anonymized, pseudonymized, deidentified, or encrypted in its definition of sensitive personal data. Data that is anonymized is by its very nature more protected than non-anonymized data and should therefore not be prohibited in the ANPRM. Safe harbors for contractually enforced anonymization requirements could also be considered.
- DOJ should offer further clarification for employment agreements in its list of covered transactions, as employment agreements are almost exclusively used within companies. The proposed inclusion of employment agreements has created considerable confusion on the applicability of DOJ's rules to companies that currently employ or are seeking to employ citizens from a country of concern.
- Access should not be included in the covered data transaction definition due to the many potential use cases. At a minimum, requirements governing access to data should only be applicable to restricted—not prohibited—transactions. Licenses for restricted access should be durable with reasonable processing timelines. DOJ should rework the definition of advertising identifiers within the definition of covered personal identifiers.
- We also seek clarity on the applicability of the rules to public traded companies that are more than 50 percent owned by companies from a country of concern, such as the US subsidiaries of Chinese companies.
- DOJ must also do more to clarify and expand the scope of exemptions for intra-entity transactions. DOJ should expand the definition of exempt intra-entity transactions to include transactions necessary for business operations, in addition to those incident and ancillary to business operations. This also includes clarifying and expanding the exemptions for "financial-services, payment processing, and regulatory-compliance related transactions" to not implicate such services that do not pose a national security threat.
- USCBC appreciates DOJ's heightened concern about government-related data and suggests that companies need not disclose data related to former government employees for compliance purposes, as doing so may inadvertently create unforeseen vulnerabilities for these individuals.
- DOJ should also clarify the applicability of its rules to cloud service providers (CSPs) and hybrid cloud providers by specifying that compliance liability rests with their clients, the data owners, not CSPs. CSPs' clients often encrypt data, a standard practice, and CSPs do not have access to data in a way that would allow them to feasibly comply with the rules as written.
- Going forward, DOJ should ensure that its rules are harmonized and do not duplicate international and subnational data privacy laws, such as the EU's General Data Protection Regulation (GDPR). Harmonization will enable companies to craft compliance mechanisms more smoothly and effectively.
- Companies will need time to implement a response to this ANPRM and its future rules, which will have significant impacts on businesses. To accommodate stakeholders' varying timelines needed to comply with the prohibitions, DOJ should consider excluding certain prohibited transactions or sub-categories of prohibited transactions from the requirements over a short- to medium timeline using a time-limited general license approach that could be narrowed in scope over time. We further suggest that DOJ set an implementation timeline of at least one year from

the adoption of a final rule and that thresholds be increased until implementation has been fully matured through notice and comment processes.

I. Definitional Concerns

Specific national security threats

USCBC understands that DOJ cannot provide all details of the national security threats it aims to mitigate through the ANPRM, and that the threats that it cites are broad and high-level. More specific information about the current and anticipated threats and how access to particular types of data would enhance those threats would help industry contribute to tailored rules that consider both national security imperatives and important considerations of business and commerce.

Anonymized, pseudonymized, deidentified, and encrypted data

The definition of *bulk U.S. sensitive personal data* includes data that is "anonymized, pseudonymized, deidentified, or encrypted." This definition greatly increases the potential number of covered data transactions which, by the very nature of their definition, have been altered to protect personal information. We suggest that DOJ explicitly provide exceptions for data that is properly anonymized, pseudonymized, deidentified, or encrypted. Encryption is an essential technical tool that is used extensively in industry and government to protect data security and privacy. In different applications, properly anonymized, pseudonymized, deidentified, or encrypted data does not present the risks the EO identifies, such as blackmail and espionage.

We encourage DOJ to adjust the definition of personal data, which will ensure that future regulations only apply to the most impactful transactions. Failure to adjust along these lines will significantly impact non-sensitive, intra-company processes including in global public health areas. For example, we are deeply concerned that the ANPRM could prohibit companies that engage in clinical trials from using anonymized clinical trial data to support the launch of clinical trials in a country of concern. More broadly, companies with operations in a country of concern, such as China, would be unable to grant their employees access to anonymized data concerning sick leave or stock options.

These methods, particularly encryption, should be considered an exception to all the ANPRM's sensitive personal data categories. We further suggest that DOJ implement a safe harbor or exclusion for anonymized data where businesses contractually bind vendors to not re-identify the data. Such an exclusion would be in line with the California Consumer Privacy Act, which excludes de-identified data if there are public and contractual commitments against a vendor re-identifying the data. DOJ should similarly add contractual commitments against re-identification to its criteria for restricted contractual obligations.

Data transactions that involve any bulk US sensitive data

The proposed definition of *covered data transaction* is broad and includes "any transaction that *involves* any bulk US sensitive personal data or government data." We seek clarification on how companies should interpret involves. For example, there are situations where the US person is an intermediary in a transaction involving bulk US sensitive data, but such intermediary services would not involve the actual transfer of the bulk US sensitive data from the data broker to a covered person because the data broker

would execute its services directly, on the covered person's behalf without transferring or disclosing the US bulk sensitive data to the intermediary. In a second example, marketing services could be delivered to covered persons without providing them with access to underlying data. Where the intermediary or a covered person does not access or receive the US bulk sensitive data, even if they are involved in the transaction, DOJ should confirm that such transactions are out of scope.

Advertising and network-based identifiers

The definition of *covered personal identifiers* is broad, and, in parts, complex and difficult to apply. For example, *covered personal identifiers* includes advertising identifiers and network-based identifiers such as IP addresses and cookies in the *listed identifiers* category. This is problematic for companies with employees and vendors in a country of concern who use ubiquitous tools such as cookies for marketing and could cause substantial business impacts to companies with branches, affiliates, or entities in a country of concern. If a single cookie constitutes a covered personal identifier, companies would essentially be required to cease processing advertising data in China. DOJ should rework the definition of covered personal identifiers by excluding these types of identifiers or including them only in certain circumstances such as through a licensing process.

Covered person as it applies to US subsidiaries of companies from a country of concern

As written, the definition of a *covered person* includes persons owned or controlled by companies from a country of concern. This definition presents significant compliance difficulties given the complex nature of businesses, including the multi-level ownership structures of large, modern companies where there are numerous investors who themselves have investors. This is particularly difficult for publicly traded companies whose foreign ownership changes frequently. The DOJ should clarify the applicability of its rules to US companies that are 50 percent or more owned by companies from a country of concern, such as the US subsidiaries of Chinese companies. Clarification will help American companies that do business with the US subsidiaries of Chinese companies appropriately scope their compliance operations. We further recommend modifying this standard to reflect that of the export administration regulations where the expectation includes a standard of knowledge.

Bulk thresholds

The decision to adopt bulk thresholds for data transactions should be reconsidered. This concept was first engineered by China to the detriment of its economy, competitiveness, and attractiveness as an investment destination. From an implementation standpoint, there are several issues with bulk thresholds. It is unfeasible for companies to decrypt encrypted data sets to calculate the number of *covered personal identifiers* in a data set for compliance purposes. Being required to do so could possibly lead to reduced data security. Furthermore, companies' reporting metrics for bulk thresholds is unclear, such as whether calculation for thresholds should be done annually versus on a per-transaction basis. At a minimum, we suggest that the DOJ substantially raise its thresholds until it has provided further guidance to industry.

The DOJ should also specify whether the bulk threshold quantitative criteria apply to each legal entity the engages in data transactions or to the total number of transactions across multiple affiliated companies. We request clarification on this point.

Geolocation and sensor-related data

The ANPRM focuses on how to technically define "precise geolocation data," but does not address the challenges companies would face in identifying all such data and handling it in accordance with the proposed rule. Precise geolocation data is used by and incorporated into a large variety of device and software services. As a result, the inclusion of such data would have a substantial impact on the cost and competitiveness of US companies. We request clarification on how companies should identify and handle geolocation data. DOJ should, at a minimum, establish a licensing process for companies that handle this data in accordance with security requirements outlined in further rulemaking.

II. Access to data as a class of restricted transaction

As written, DOJ's inclusion of *access* in the definition of covered transaction encompasses innumerable business scenarios. Many US companies rely on individuals outside the United States to access and process data as part of their day-to-day operations. The inability of some employees to access data will adversely affect these companies by introducing complexities that could result in substantial product delays, reduce their ability to innovate, and impede their ability to leverage global talent. We suggest that the DOJ remove *access* from the definition of *covered data transaction.* Doing so will help create a regulatory system that is appropriately scoped to cover the most impactful transactions.

At a minimum, *access* should only be subject to requirements for restricted transactions, not prohibited transactions. Compliance processes for clearing *access* under restricted transactions should be based on a detailed standard, such as security measures outlined in NIST or CISA guidance, to mitigate risks while allowing exclusions. A separate standard for *access*, unlike transfer, should be established because *access* can more easily be disabled. For example, certain companies use corporate intranet where outbound transfer is impossible. Companies also deny access to relevant datasets for employees in countries of concern that separate from the company. To the extent that risk is too high, DOJ could establish a licensing process for these activities. Licenses should have a four-year validity period like the export administration regulations and permit multiple transactions under a single license.

Like our points below on employment agreements, regulations mandating that projects with sensitive data can only be performed by employees based in certain countries will significantly limit how global companies can deploy and utilize talent. This will further complicate hiring, budgets, and product rollouts and could harm innovation. Companies' internal security and privacy programs often follow NIST guidelines and other international standards, and we suggest that intra-company exemptions be tailored in such a way that freely enables companies to utilize global talent.

III. Exemptions for Intra-entity Transactions

The ANPRM exempts intra-entity transactions between a US person and its subsidiary or affiliate that is subject to the jurisdiction of a country of concern when such transactions are "incident to" business operations that are "ancillary." The proposed text and examples leave the limits of "ancillary" operations unclear and unduly burden necessary transactions. DOJ should expand its definition of excluded intra-entity transactions to include necessary transactions, such as transactions "necessary, incident, and ancillary to marketing operations, business efficiency operations, product improvement operations, cross-border innovation, and operations to facilitate efficiencies or begin certain activities in a country of concern." By providing robust exclusions for intra-company transactions, the DOJ can ensure that its rule

is minimally disruptive to multinational companies and does not inadvertently foment data localization practices.

If the DOJ cannot expand exclusions for intra-entity transfers, it should consider establishing a licensing process to allow for additional intra-entity transfers that are necessary to conduct routine business operations. At a minimum, we urge the DOJ to provide further clarity in the rule on what constitutes "ordinary and incident to and part of ancillary business operations."

For example, we would welcome clarification that if a US person or company has a subsidiary or office in a country of concern, the proposed rule would not prevent a foreign person employee in that subsidiary or office from accessing information such as the company staff directory. We further seek confirmation as to whether the intra-entity transactions exemption would also apply to subsidiaries in countries of concern and should also extend to intragroup transfers made between multinational companies, joint ventures or partnerships, business associates, and affiliates that share personal information in the normal course of business. The risk of personal data mishandling and misuse is generally lower for intragroup transfers. These transactions are within and between entities (for example, foreign branches) of a US company, in which all entities are under a single control and management structure and bound by the same centrally applied and approved privacy policies and procedures.

Exemptions for Employment Agreements

DOJ should specify that employment agreements are included in its list of exempted intra-entity transactions. Employment agreements are inherently intra-company and, as suggested above, should be included in a greater set of exclusions for intra-entity transactions that must be permitted to allow global company operations to continue. Companies from nearly all sectors utilize employment agreements in China and will be significantly impacted by employment agreements if they are included as covered data transactions.

The final rule should also make clear that intra-company exemptions cover all employees of an affiliated entity in a country of concern, all affiliated entities in a country of concern subject to relevant aspects of control by the US entity, and all transactions conducted by a service provider that the US person is authorized to control. This would include low risk routine practices such as financial accounting, human resources, and recruiting. As the DOJ, the Department of Commerce, and the Director of National Intelligence stated in their 2020 White Paper on privacy safeguards and data transfers, most entities do not work with data that is "of any interest" to US intelligence agencies.

In that same vein, given how the ANPRM is written, it is unclear under what circumstances the security requirements could allow a US company to employ a Chinese citizen in the United States to do work involving bulk US sensitive personal data or US government data. It is also unclear in the ANPRM when the security requirements will be clarified relative to the promulgation of the final rule. Employment agreements typically involve applications for visas, offers of employment, and major life decisions as to whether an individual moves to the United States. Also, from the employer's perspective, employment agreements involve training for and investment in particular individuals that are hired for particular roles. Given these factors, the DOJ should clarify when it intends to publish the security requirements and provide more detail on how companies' implemented security policies might permit companies with bulk US sensitive personal data or US government data to employ Chinese citizens.

Exemptions for financial services

USCBC and its members welcome the exemption of financial services, payment processing, and regulatory compliance-related transactions. In this regard, the rule was carefully scoped to enable seamless business and commercial transactions while recognizing that disclosing data in the provision of such services does not pose an unacceptable risk to the national security of the United States. However, USCBC recommends refining the exemptions to paragraphs (i) – (iv) of the section "financial-services, payment processing, and regulatory-compliance related transactions." Our suggested revisions are in ***Bold & Italics*** below:

> *(i) Banking, capital-markets, or financial insurance services;*
>
> *(ii) An activity authorized **for national banks** by 12 U.S.C. 24 (Seventh) and rules and regulations **and written interpretations of the Office of the Comptroller of the Currency** thereunder;*
>
> *(iii) An activity that is ''financial in nature or incidental to a financial activity'' or ''complementary to a financial activity,'' as set forth in section 4(k) of the Bank Holding Company Act of 1956 and rules and regulations **and written interpretations of the Board of Governors of the Federal Reserve System** thereunder;*
>
> *(iv) The provision or processing of payments involving the transfer of personal financial data or covered personal identifiers for the purchase and sale of goods and services (such as the purchase, sale, or transfer of consumer products and services through online shopping or e-commerce marketplaces); **the provision or processing of funds transfers (such as person-to-person, business-to-person and government-to-person funds transfers) involving the transfer of personal financial data or covered personal identifiers; the provision of services ancillary to processing payments and funds transfers (such as services for payment dispute resolution, payor authentication, tokenization, payment gateway, payment fraud detection, payment resiliency, mitigation and prevention, and payment-related loyalty point program administration);** other than data transactions that involve data brokerage; and*

IV. Government-Related Data

USCBC appreciates the need to protect government-related data, including that of current and former US Government officials, military personnel, and contractors. However, as written, the ANPRM will be challenging to implement. Companies may not know which employees are former US government officials or contractors, especially those who are former military or formerly a member of the intelligence community. US companies requesting this data from their employees may create a database of sensitive information and individuals that bad actors could target, increasing the attacks against companies. We recommend that the DOJ change this requirement to protect the data of former US government officials, military personnel, and contractors who have identified themselves as such.

The ANPRM defines government data as "any precise geolocation data, regardless of volume, for any location within any area enumerated on a list of specific geofenced areas associated with military, other government, or other sensitive facilities or locations (the Government-Related Location Data List)."

While the definition is broad, the DOJ should clarify that companies not engaging in the sale of such data are not covered, consistent with examples 10 and 11 from the ANPRM.

V. Exemptions for Cloud Service Providers

Liability for cloud service providers

Executive Order (EO) 14117 and the ANPRM do not define how liability will apply between a Cloud Service Provider (CSP) and its client, the data owner. Most CSPs define data ownership and control parameters in their client contracts. Clients therefore typically maintain ownership and control of their data while utilizing a CSP's cloud infrastructure and services. Often, a client will encrypt the data and maintain the encryption keys, meaning the CSP does not have the technical ability to access the data. As currently written, EO 14117 would require that a US CSP modify its behavior with respect to data gathering/meta data collection and transfers, irrespective of whether the CSP is the ultimate data owner.

DOJ should clarify, therefore, that liability to comply with EO 14117 rests with the data owner, not the CSP. This can be done by revising the definition of "data brokerage" to clarify that third party service providers are exempt from liability to the extent that they are merely offering a platform for use by customers. Moreover, any final rule should clarify the minimum threshold value for data transfers when no liability would be incurred by the data owner. Lastly, the final rule should clarify with which organization liability applies to, particularly regarding downstream non-compliance (e.g., if companies insert requirements into their contracts with third parties and those third parties fail to meet these requirements, those third parties, not the CSP, should be held accountable). Our suggested revisions to the definition of "data brokerage" are in bold and italics below:

> *The sale of,licensing of access to, or similar commercial transactions involving the transfer of data* ***directly*** *from any person (the* ***data*** *provider) to any other person (the* ***data*** *recipient),* ***whether or not by means of a third-party service,*** *where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data.* ***For avoidance of doubt, a third-party service provider does not engage in data brokerage solely by providing a platform upon which a data provider conducts such a transaction with a data recipient.***

Liability for hybrid cloud

Most companies today rely on multiple cloud provers and platforms to manage their infrastructure and data operations. "Hybrid cloud" combines and unifies public cloud, private cloud and on-premise infrastructure to create a single, optimal IT infrastructure. As a result, a company will contract with multiple cloud vendors to manage, move, and handle data. Given this reality, the final rule implementing the EO should allocate responsibility for compliance to the entity that owns and controls the data and clarify that liability for implementation and enforcement of the EO rests with the data owner, not the CSPs providing hybrid cloud infrastructure and services.

VI. U.S. and International Harmonization

USCBC recognizes that the EO and the ANPRM are national security regimes, not privacy regulations. Much of what the EO and ANPRM would regulate, however, is also subject to a variety of US state and potentially federal privacy legislation. Companies have implemented compliance programs consistent with those requirements. The ANPRM risks imposing a second, inconsistent set of rules that could cause confusion and misinterpretation, which could complicate compliance efforts.

DOJ should consider the restrictions and requirements of other foreign and US jurisdictions when imposing restrictions on US companies that conduct international data transactions. The European Union's General Data Protection Regulation (GDPR), for example, includes standard contractual clauses, transfer impact assessments, and technical organizational measures. If DOJ's approach were more aligned with other international commitments, it would allow companies to create harmonized compliance mechanisms across jurisdictions. Similarly, DOJ should consider how best to align with existing US privacy frameworks (e.g., under the various state privacy laws), and make use of existing definitions and concepts where possible to increase regulatory clarity and reduce compliance burdens for entities covered by the ANPRM.

VII. Efficacy, Implementation, and Due Diligence

Balanced against the considerable costs the ANPRM would impose upon US businesses that rely on cross-border data transfers, it is not clear that the proposed regime would effectively mitigate the threat that countries of concern present. For example, it is not clear how the ANPRM would affect the resale of U.S. person data by a non-U.S. person company to a covered person, or how a U.S. seller could detect a covered entity that has obfuscated its identity, such as through a VPN or a front company.

Moreover, companies will need time to implement a response to any final rule as well as any other future regulations governing bulk data transfers to countries of concern and integrate their responses into extant compliance programs. For example, certain vendor and employment agreements may need to be updated; business processes will need to be changed; and any operational changes will need to be engineered and tested. Given the complexity, we believe that the implementation timeframe should be **at least one year** from adoption of a final rule. We suggest that any future regulations under the auspices of this program maintain a risk-based approach. We also note that any across-the-board mandates would create significant, potentially duplicative compliance obligations for companies with unique risk profiles.

USCBC appreciates the opportunity to comment on this ANPRM and hopes to continue to work with the administration to craft policies that are effective, narrowly tailored in scope, multilateral and flexible and that promote companies' ability to leverage global data flows. Doing so would help US companies maintain their global competitiveness. We hope to help the DOJ craft a strategy that balances the administration's security priorities with the technological efficiencies inherent to the operations of companies that rely on cross border data transfers.