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 Notice of Proposed Rulemaking (NPRM) 89 FR 86116 (October 29, 2024), outlining the proposed implementation of the regulations contemplated by the Executive Order (EO) 14117 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 in 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, life-sciences, technology, financial services, and others.

As raised previously in our ANPRM submission to the DOJ, USCBC supports the US government's efforts to protect Americans' sensitive personal and government related data. Today's interconnected and digital world requires a shared determination between the public and private sector to stop malicious actors from harming American citizens and entities.

USCBC commends the DOJ for incorporating certain key proposals from our ANPRM submission. We support the inclusions of exemptions for corporate group transactions to maintain business continuity, particularly between a US parent company and its subsidiary in China. We also endorse the new exemptions for telecommunications, certain health data, and pharmaceutical and medical device authorizations. These measures will help more easily facilitate commercial transactions and advance healthcare for US patients, reflecting the low national security risk posed by data disclosures for these purposes, while also ensuring that US firms are given the flexibility needed to pursue commercial opportunities in crucial growth areas and deliver innovative healthcare products.

However, USCBC is concerned that many elements of the proposed rule are overly broad or lack appropriate definitional refinement needed for business compliance. USCBC strongly supports further refinement of specific definitions, outlined in our letter, as doing so will ensure that the rules do not impact a swathe of business activities beyond their intended purview. Additionally, upward adjustments to the thresholds are urgently needed to reflect the rulemakers' nuanced intent to regulate "bulk transactions" and to enable regulators to focus on the most impactful data transfers. This is especially critical concerning the NPRM's definitions of "human genomic data," "human biospecimens," "clinical trials," "sensitive personal data," and "data brokerage." USCBC also recommends expanding the exemption for corporate group transactions and clarifying exemptions related to employment and financial services. Without such refinements, the rule risks impeding routine operations and public health initiatives aimed at protecting and improving the health of Americans. We urge DOJ to proactively engage with industry as it further refines the proposed data restrictions.

In our comments below, USCBC strives to act as a resource to the DOJ. Our submission provides specific feedback on key definitions, concepts, and elements posed in the NPRM.

I. Refine Key Definitions

A. *Narrow the definition of genomic data*

USCBC is concerned that the definition of "human genomic data" is overly broad, encompassing all 'omic data. This expansive definition is concerning since there are varying levels of data sensitivity and identifiability associated with different types of 'omic data. Not all 'omic data carries the same risk of re-identification or misuse, and treating all such data uniformly may unnecessarily hinder legitimate research, clinical practices, and regulatory activities.

USCBC recommends that DOJ narrow the definition of "human genomic data" by providing specific, finite examples of what types of human genomic and other 'omic data are included. Less sensitive 'omic data should also be defined and excluded from the regulatory scope. Additionally, we suggest increasing the bulk threshold for genomic data transactions to 10,000. Raising the threshold would ensure that only the most impactful transactions are covered by the regulations, right-sizing the compliance burden for enterprises and focusing government bandwidth on transactions with higher risks. Alternatively, DOJ should consider adding a "substantial" modifier to its thresholds for less sensitive 'omic data that is defined by a higher threshold. Given the complex technical issues involved and the potential impact on healthcare, DOJ should consult with relevant US agencies and industry sectors before finalizing these rules.

B. *Limit the definition of human biospecimens*

The definition of "human biospecimens" also is similarly broad, encompassing not only raw human samples but also finished biological products such as cell therapy products and certain human blood products. This expansive definition prohibits these transactions and as a result could impede the development, manufacture, and distribution of essential medical treatments consisting of these products. USCBC proposes that DOJ limit the definition of "human biospecimens" to raw human samples and affirmatively exclude finished medical product primary materials and samples that are processed (in whole or in part) in finished biological products.

C. *Clarify the meaning of "relate to an individual" within the context of sensitive personal data*

Under the proposed rule, sensitive personal data is defined to exclude data "that does not relate to an individual." As drafted, this provision would exclude precise geolocation information about a device from the scope of the rule when it "does not relate to an individual." However, the DOJ does not clarify what it means for information to "relate to an individual." Specifically, it does not explain whether information would "relate to an individual" if it could be connected to a person when combined with another data set. To avoid confusion, USCBC recommends DOJ either define the phrase "relate to an individual" or provide a clarifying example that makes clear that the information does not "relate to an individual" merely because it can be associated with an individual with access to a separate data set.

D. *Anonymized clinical trial data should be excluded*

While we commend the exclusion of regulatory approval data and clinical investigations data from the definition of covered data, we find the specific exclusions on clinical trial data are not

broad enough for meaningful utilization by industry. As noted in our ANPRM submission, we were concerned that the ANPRM could prevent companies that engage in clinical trials from using anonymized clinical trial data to support the launch of clinical trials in a country of concern. This issue remains unaddressed in the NPRM. Anonymized clinical trial data should be explicitly added to the clinical trials exclusion in the final rule or any additional iterations.

E. *The clinical trial data exclusion should encompass the use of third-party vendors and affiliates*

As written, the proposed regulations prohibit the use of third-party vendors and affiliates to assist with data submissions necessary for approvals in a country of concern. Similarly, for clinical investigation and post-marketing surveillance data, the exclusion is limited to FDA-regulated investigations, thus restricting its scope and potentially impacting studies involving real-world data and evidence not regulated by the Food and Drug Administration. Instead, the DOJ should broaden the definition of excluded clinical trials to include research on biological products and medical devices conducted in compliance with FDA's Good Clinical Practice (GCP) guidelines.

Local resources are necessary because every country has specific submission requirements that are best understood by local experts and often submissions must be made by a local agent. Submissions must also be made in the local language with the support of local personnel best suited to develop submission documents and supporting material.

F. *Clarify the scope of data brokerage*

The DOJ defines "data brokerage" more broadly than the common understanding of a data broker. In the proposed rule, it is defined as "the sale of data, licensing of access to data, or similar commercial transactions involving the transfer of data from any person (the provider) to any other person (the recipient), where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data."

Multinational corporations often have multiple legal entities that share personal data. The "recipient" of that data may be a corporate affiliate that accesses, stores, or processes that data on behalf of the US "provider" more efficiently or effectively than the provider can, just as an outside vendor might do. However, it is not clear whether a multinational corporation's global data sharing agreement would potentially be covered as a "similar commercial transaction." A conservative reading of the rule could prohibit any access by or transfer to a country of concern, even when the transaction might merely be restricted if it were pursuant to a vendor agreement.

DOJ should clarify that "data brokerage" does not include intracompany transfers and service provider/vender transfers that do not involve a sale or license to access covered data or otherwise give the recipient a "right, remedy, power, privilege, or interest with respect to" the data. Additionally, USCBC recommends DOJ limit the definition of "data brokerage" to only sales of data as a transaction.

G. *Rework the scope of advertising and network-based identifiers*

The definition of covered personal identifiers remains broad and difficult to apply. It includes advertising identifiers and network-based identifiers like IP addresses and cookies. Many

cookies contain advertising IDs, meaning that a single cookie could like information and become a covered personal identifier for the purposes of covered data transactions. This inclusion is problematic for companies with employees or vendors in countries of concern who use ubiquitous tools like cookies for marketing purposes, potentially causing substantial business impacts to companies with branches, affiliates, or entities in such countries.

For example, a company using a vendor to target customers in China could be engaged in a covered data transaction if it provides the vendor access to marketing data of US citizens to analyze trends for creating marketing campaigns. This would include allowing access to those data sets by marketing employees in a country of concern, which could inadvertently harm legitimate business activities.

We recommend that the DOJ rework the definition of covered personal identifiers by excluding advertising and network-based identifiers or including them only in certain circumstances, such as through a licensing process. Additionally, we ask for an exception for intra-entity transactions that would facilitate innovation and cross-border efficiencies for global companies. By adjusting these definitions and exemptions, the DOJ can ensure companies are not unnecessarily restricted from processing advertising data or engaging in legitimate business operations.

II. Broaden and Clarify Exemptions

A. *Expand corporate group transactions*

USCBC is encouraged by the NPRM's exemption for corporate group transactions between a US person and its subsidiary or affiliate under the jurisdiction of a country of concern, provided such transactions are "incident to" and "ancillary" to business operations. However, the requirement for companies to implement additional access protocols -- limiting employees in countries of concern to pseudonymized, anonymized, or de-identified data -- presents substantial challenges. These protocols complicate the operations of multinational companies that depend on integrated data systems and cross-border collaboration for efficient functioning.

Implementing these additional access protocols will also be costly and burdensome. Biopharmaceutical manufacturers, for example, already have strong security and data governance measures in place to protect sensitive information. They utilize intra-affiliate data transfer agreements and other transfer mechanisms to safeguard data between affiliates. Moreover, these companies often have contractual or legal obligations to comply with when storing and protecting data, which may include adherence to international standards and best practices that meet or exceed the NPRM's objectives.

Requiring companies to overhaul their existing security frameworks to comply with new access protocols may lead to operational disruptions without providing commensurate security benefits. The additional costs and resource allocations could divert attention from core activities such as research and development, ultimately impacting innovation and competitiveness. It is important to recognize that these companies are already deeply invested in maintaining the highest levels of data security due to the sensitive nature of their work and the regulatory environments in which they operate.

We recommend that the DOJ expand the exemption for corporate group transactions to encompass a broader range of necessary business activities beyond routine administrative

support, such as transactions "necessary, incident, and ancillary to marketing operations, business efficiency operations, product improvement operations, cross border innovation, global operations of a service related to US persons, and operations to facilitate efficiencies or begin certain activities in a country of concern."

We also recommend supporting this expansion with additional examples, such as, "A US company that is a financial services provider has a foreign subsidiary located in a country of concern. Customers of the US company conduct financial transactions in the country of concern and customers of the foreign subsidiary conduct transactions in the US. The foreign subsidiary accesses bulk US sensitive personal data, more particularly personal financial data, from the US company to perform customer service functions related to these transactions. This is an exempt corporate group transaction."

Furthermore, we urge the DOJ to acknowledge and accept existing security and data governance measures employed by companies as sufficient to meet the NPRM's requirements. By doing so, the DOJ can achieve its national security objectives without imposing undue burdens on businesses that are already committed to safeguarding sensitive data.

B. *Clarify employment agreements exemptions*

In USCBC's ANPRM submission, we encouraged the DOJ to specify that employment agreements are included in its list of exempted intra-entity transactions. Employment agreements are inherently intra-company and, as noted 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. We also highlighted that intra-company exemptions should 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. It was also unclear in the ANPRM 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.

While the NPRM provides certain clarifications, we respectfully request additional clarification regarding exemptions related to employment, particularly for instances where Chinese nationals are employed in the United States and go through the immigration process. As currently drafted, the NPRM also continues to impose substantial constraints on employment agreements in countries of concern, potentially creating compliance challenges that extend beyond US jurisdiction. These restrictions could hinder the legal structuring of employment agreements, which must also adhere to foreign regulatory requirements. We urge the DOJ to consider adjustments to these proposed regulations to avoid conflicts with foreign data protection laws and ensure their balanced application, thereby mitigating unnecessary compliance burdens for multinational employers.

C. *Refine the exemption for drug, biological product, and medical device authorizations*

USCBC commends the exemption for drug, biological product, and medical device authorizations. However, regulatory approval data is limited to de-identified data and the rule does not define de-identified data nor set forth standards for de-identification. The exemption also only includes data that is reasonably necessary for a regulatory authority to assess the safety

and effectiveness. The DOJ further does not consider transactions with a vendor to be "reasonably necessary."

USCBC recommends that de-identification be consistent with the FDA standards for post-marketing de-identification and include key coded data, which is used in clinical trials. This aligns with DOJ's stated aim of the exemptions covering data typically required by the FDA. We recommend the DOJ also not adopt a bright-line rule or categorically define what data might be reasonably necessary. In some foreign jurisdictions, manufacturers may be required to use a local agent when submitting for regulatory approval. The exemption should include these vendor and affiliate transactions.

D. *Clarify the scope of the financial services exemption*

1. *Make amendments to capture the broad nature of regulators*

Financial institutions operating internationally are often required to comply with requests from foreign regulators or law enforcement authorities that are lawful under the laws of the country of concern. This may include providing access to bulk sensitive personal data of US persons who are residing in or conducting transactions within that country. Such activities are integral to conducting business and complying with local legal requirements. Not being able to respond to these lawful requests would place companies in a conflict of laws position, forcing them to choose between violating US regulations or the laws of the country in which they operate.

USCBC believes that further clarification is needed to ensure that the financial services exemption adequately covers the broad nature of regulators and the legal obligations of financial institutions operating in countries of concern. Specifically, we seek confirmation that responding to lawful requests from regulators or law enforcement authorities in a country of concern is considered "ordinarily incident to the provision of financial services" and is therefore exempt under the rule.

USCBC recommends that the DOJ amend the financial services exemption highlighted by Example 10 to reflect this clarification by using the following language:

"A US financial services provider operates a foreign branch, subsidiary, or affiliate in a country of concern and provides financial services to US persons living within or visiting the country of concern. The financial services provider, its foreign branch, subsidiary, or affiliate receives a request which is lawful under the laws of the country of concern from a regulator or law enforcement authority in the country of concern to review the financial activity conducted in the country, which includes providing access to the bulk sensitive personal data of US persons resident in the country or US persons conducting transactions through the foreign branch, subsidiary, or affiliate. Responding to the request of the regulator or law enforcement authority, including providing access to this bulk sensitive personal data, is ordinarily incident to the provision of financial services and is exempt."

2. *Clarify that data transfers may be required reactively in relation to a government request as part of routine reporting requirements*

Financial institutions operating in countries of concern often have mandatory reporting requirements imposed by local regulators or law enforcement authorities. For instance, quarterly reports or ad hoc information requests related to China inbound transactions (such as US persons or cardholders transacting at a Chinese merchant) may need to be submitted to authorities like the State Administration of Foreign Exchange or the People's Bank of China

(PBOC, the Central Bank). These reports are required under the laws, regulations, or guidance of the country of concern, and compliance is essential for lawful operation. USCBC recommends including an additional example to complement the financial services exemption in Example 11 which clarifies that data transfers may be required not only reactively in response to government requests but also as part of routine reporting obligations.

Recommended language to consider:

"A US financial services provider operates a foreign branch, subsidiary, or affiliate in a country of concern and provides financial services to U.S. persons living within or visiting the country of concern. The financial services provider, its foreign branch, subsidiary, or affiliate is subject to reporting requirements imposed by a regulator or law enforcement authority with jurisdiction over it in the country of concern. Compliance with these reporting requirements includes providing access to the bulk sensitive personal data of US persons resident in the country or US persons conducting transactions through the foreign branch, subsidiary, or affiliate. Complying with the regulator's reporting requirements, including providing access to this bulk sensitive personal data, is ordinarily incident to the provision of financial services and is exempt."

3. *Clarify that cybersecurity services may be considered ancillary to processing payments*

Cybersecurity measures are essential components of modern payment processing, designed to prevent or identify potentially fraudulent or nefarious cross-border transactions. Recognizing these services as ancillary ensures that companies can continue to provide critical protections without unintended regulatory burdens. USCBC suggests including an additional example to clarify that cybersecurity services may be considered ancillary to processing payments and funds transfers, particularly as forms of risk mitigation and prevention.

The new example would be as follows:

"A US company that provides payment-processing services for cross-border payment transactions sells cybersecurity services to financial institutions, merchants, and other payment recipients that are incorporated in, located in, or subject to the jurisdiction of a country of concern. The services are ancillary to the payment processing and are designed to prevent or identify potentially fraudulent or otherwise nefarious cross-border payments to such parties. To provide the services, the US company engages in data transactions to transfer bulk sensitive personal data such as IP addresses, email addresses, and device information, along with financial data, to such parties. Both the US company's transaction transferring bulk sensitive personal data and the payment transactions by US individuals are exempt transactions."

4. *Clarify the inclusion of product development*

USCBC recommends adding a new example to clarify that product development may be considered "ordinarily incident to and part of the provision of financial services." Example 4 of the financial services exemption indicates that sending bulk personal financial data for the purposes of developing a financial software tool is not ordinarily incident to and part of administrative or ancillary business operations. However, product development is integral to providing financial services, especially in the development of fraud detection and cybersecurity services within the global payment ecosystem.

Fraud trends that emerge in one region or country can quickly spread to others. To build effective fraud detection and prevention models and gain necessary insights into fraudulent activities, these models must be developed using global or multi-country data sets. Analyzing data collectively is essential for spotting patterns of fraud; excluding data from certain regions would deprive the models of the training required to accurately detect and prevent fraud. We suggest the following language:

"A US financial services provider transfers US bulk sensitive data to a foreign branch, subsidiary, or affiliate located in a country of concern as ordinarily incident to and part of the process of developing or improving its financial products and services. The transfer is exempt."

III. Recommended Practices for Efficacy, Implementation, and Due Diligence

Moreover, it appears the proposed obligations may extend beyond CISA's requirements, thus imposing further compliance challenges. This proposal would coincide with pre-existing regulatory obligations, amplifying the burden on organizations that already maintain rigorous compliance programs, comprehensive security protocols, and data governance practices. For entities operating in highly regulated fields, such as those subject to drug, biological product, and medical device authorizations, the proposal's requirement to file reports—even when relying on these specific exemptions—presents an unnecessary burden. This is particularly true given that these entities are already required to maintain detailed transaction records, which are readily available upon request under current compliance frameworks.

With this in mind, USCBC recommends a phased implementation approach for any finalized rule, with full compliance set to commence no sooner than one year from the rule's adoption. Such a timeline would provide US entities with adequate time to achieve full compliance while effectively managing unanticipated business expenses, cybersecurity measures, and enhanced record-keeping requirements. A phased approach would mitigate the immediate operational impact and allow for a gradual adjustment period, ensuring that compliance obligations are met without unduly straining resources or compromising existing programs.

Regarding the need for contractual restrictions in data brokerage transactions with foreign persons, the DOJ should also clarify that the NPRM does not apply to agreements entered into prior to the effective date. If the DOJ determines that the regulation applies to agreements entered into prior to the effective date, we request that the DOJ provide for an effective date that allows sufficient time for US companies to amend existing agreements.

A. *Harmonize system-level security requirements*

As understood in the NPRM, restricted transactions involve access to covered data by covered persons. The intent of the CISA security requirements is to establish conditions under which such restricted transactions may go forward, not prohibit them entirely. Under the proposed rule, no US person may engage in a covered transaction "unless the US person complies with the security requirements [promulgated by DHS]" and a transaction is "covered" if it "involves any access" to covered data by a covered person. If the true intent of the DOJ is that the CISA security requirements allow access to covered data by covered persons under certain circumstances, the rule, as written, would not accommodate for that. This is because if covered persons never have access to any covered data, the transaction would no longer be "covered" by

the rule, and none of the security requirements would apply. USCBC recommends adding the word "unauthorized" before access to accomplish the intent of ensuring covered systems are sufficiently secure and that system owners can regulate which persons, including covered persons, have access to covered data and under what conditions.

B. *Clarify between inclusion and exclusion criteria*

Restricted transactions are allowed if certain security controls are put in place. However, the security controls, when considered alone, would prevent the transactions from occurring. For example, the security controls require limiting access to prevent countries of concern and covered persons from gaining access to the covered data. But if an employee of a global company working in China needs to process bulk sensitive data, they must access the data. This would be a violation of the security control requirements, effectively blocking the transaction. For restricted transactions to have meaning, the security controls must be read in a manner such that the covered persons and countries of concern mentioned are outside of the intended recipient.

USCBC appreciates the opportunity to provide feedback on this NPRM and to be consulted throughout the rulemaking process. The administration's intent to foster industry collaboration is not only beneficial to affected stakeholders but also ensures that the final rule strikes an essential balance among national security, economic interests, and public health. USCBC encourages DOJ and relevant interagency stakeholders' to continue to engage with industry. Such a collaborative effort is essential to effectively implement complex regulations such as this. USCBC looks forward to continuing to serve as a resource for DOJ as this process advances, contributing insights to support an effective, balanced regulatory framework.