BR Business Roundtable

1000 Maine Avenue, SW, STE 500
Washington, DC 20024
202.872.1260
brt.org

April 19, 2024

U.S. Department of Justice
National Security Division, Foreign Investment Review Section
175 N Street, NE, 12th Floor
Washington, DC 20002

RE: Comments on 89 Fed. Reg. 15780 (March 5, 2024); RIN 1105-AB72; Docket No. NSD 104

The Business Roundtable (BRT) submits these comments in response to the Advance Notice of Proposed Rulemaking (ANPRM) from the National Security Division of the Department of Justice (DOJ).[1] BRT appreciates the opportunity to comment on the DOJ's proposed regulations that restrict U.S. persons from engaging in certain data transactions.

BRT is an association of more than 200 chief executive officers (CEOs) of America's leading companies, representing every sector of the U.S. economy. BRT CEOs lead U.S.-based companies that support one in four American jobs and almost a quarter of U.S. GDP.

BRT and its members take data privacy seriously and recognize the national security interests implicated by data privacy and security. BRT member companies invest heavily in privacy and security safeguards designed to protect sensitive information and implement robust compliance programs. Regulatory requirements should be appropriately scoped to address national security risks while avoiding unnecessary impacts on business operations, customer services or global competitiveness. For this reason, BRT urges the DOJ to tailor the proposed rules to focus on the data elements and transactions that are most likely to create material risks to Americans and national security, while avoiding unnecessary disruption of routine business operations. Additionally, BRT urges Congress to consider responses to this ANPRM when developing legislation that includes similar definitional and jurisdictional concerns.

Below, BRT answers key questions posed by the ANPRM.

I. Treatment of Anonymized, Pseudonymized, De-Identified or Encrypted Data [ANPRM Q2]

The ANPRM asks if the DOJ should treat data that is anonymized, pseudonymized, de-identified or encrypted differently.[2] We recommend that the regulation treat data protected via

[1] U.S. Department of Justice, Advance Notice of Proposed Rulemaking on Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern, 89 Fed. Reg. 15780, Mar. 5, 2024, https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and.
[2] 89 Fed. Reg. 15786 (2024).

encryption, anonymization, de-identification or pseudonymization differently from cleartext or plaintext data.[3] While the precise definition of anonymous versus pseudonymous data can be fluid and inconsistent across industries, what is clear is that all de-identified or encrypted data is more secure than cleartext or plaintext data. When properly implemented, these techniques can mitigate the privacy and security risks of data to varying degrees.[4] Businesses rely on encryption anonymization and pseudonymization to securely transfer data, counter fraud and carry out other operational activities that are fundamental to modern commerce.

We recommend the DOJ continue to promote the use of strong encryption, de-identification and, in particular, anonymization as part of its overarching data protection strategy. Encryption, anonymization and de-identification are crucial tools that the business community relies on to enable global data flows while protecting the underlying data and preserving storage and transfer capabilities. Virtually all privacy regulatory frameworks provide flexibility regarding restrictions on such data due to the lower risk of association with individual identities. For example, while the Health Insurance Portability and Accountability Act (HIPAA) protects the privacy and security of individually identifiable health information,[5] the HIPAA Privacy Rule also provides a specific Safe Harbor for de-identified data.[6] Many international jurisdictions consider truly anonymized data as non-personal data and therefore exclude it from data protection requirements.[7] Further, the ANPRM proposes encryption as one of the four security conditions permitting "restricted transactions" (Section I), indicating that encryption is a security control sufficient to mitigate national security risks.[8]

As such, anonymized, pseudonymized, de-identified or encrypted data should be excluded from the definition of "bulk sensitive personal data" if effective processes are implemented to prevent re-identification (e.g., measures to keep the encryption key confidential, securing related data sets). The DOJ should recognize internationally accepted industry standards for anonymization, pseudonymization, de-identification and encryption that provide a high level of

---

[3] De-identification is an umbrella term that includes anonymization and pseudonymization. National Institute of Standards and Technology, De-Identification of Personal Information, NISTIR 8053, Oct. 2015, https://nvlpubs.nist.gov/nistpubs/ir/2015/nist.ir.8053.pdf.

[4] We recognize that pseudonymization may be technically reversible and thus may not merit the same treatment as encrypted and anonymized data.

[5] 42 U.S.C. 1302d(6) and 45 CFR 160.103.

[6] 45 CFR 164.514(b). See also U.S. Department of Health and Human Services, Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html.

[7] See, for example, Recital 26, General Data Protection Regulation, Regulation (EU) 2016/679. *The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.*

[8] 89 Fed. Reg. 15795 (2024).

privacy and security protection, including the standards with which financial institutions and health care covered entities are already subject.

This interpretation is also consistent with the proposed definition of "access" which covers ''logical or physical access, including the ability to obtain, read, copy, decrypt, edit, divert, release, affect, alter the state of, or otherwise view or receive, in any form, including through information-technology systems, cloud-computing platforms, networks, security systems, equipment, or software.''[9] If data is encrypted in such a way that the covered person does not control and does not have access to encryption keys, such data should not be regarded as accessible. Alternatively, we recommend the Department of Justice clarify that encrypted U.S. bulk sensitive data where a U.S. person controls the encryption key and the keys are managed outside the country of concern is not in the scope of the definition.

Similarly, anonymized data is, by definition, data that has rendered an individual "unidentifiable." Anonymization techniques enable data to be leveraged for analysis and insights, help protect trade secrets and intellectual property, and prevent competitors from accessing sensitive information while protecting individuals by preventing their identification. The ANPRM itself acknowledges the benefits of anonymized data by identifying classes of listed identifiers and the rules on their combination that aim to identify an individual from a data set or link data across multiple data sets to an individual. However, this guidance appears in direct contradiction with a proposal to wholesale include "anonymized" data within the definition. We therefore recommend either excluding the definition of "anonymized data" or providing greater clarity as to what types of anonymization techniques pose a greater national security risk and would be outside of the scope of the definition.

II. Determining Bulk Thresholds [ANPRM Q7-9]

The ANPRM asks what bulk thresholds should apply for categories of covered data, as well as what additional factors and use cases should be evaluated as part of the framework to determine bulk thresholds.[10] BRT recommends a risk-based approach to setting the bulk thresholds that considers: (1) the risks to national security associated with countries of concern or covered persons accessing the sensitive information; and (2) the business utility of storing or transferring the information in a data-driven global economy.

The first consideration should include the risk that the data identify or link to specific individuals. Some categories of covered information pose a greater risk of association with an identifiable individual than other categories. For example, biometric identifiers are more likely to be linked to an identifiable individual than personal health data stripped of identifiers.

[9] 89 Fed. Reg. 15788 (2024).
[10] 89 Fed. Reg. 15787 (2024).

With regard to business utility considerations, it is important to note that the ANPRM envisions not just restrictions on sales of bulk sensitive information with countries of concern and covered persons but also imposes privacy and security requirements for commercial agreements that may involve a risk of access to such information.[11] Collection and storage of covered data at higher volumes is increasingly common for a variety of business, technical and administrative purposes, including among entities that do not intend to sell or transfer such data to countries of concern or covered persons.

In recognition of clear trends towards storage of larger volumes of data for legitimate business purposes that do not pose national security risk, BRT believes higher bulk thresholds are appropriate. In considering the thresholds, the DOJ should consider use cases where covered data is used to provide services that Americans value and that strengthen the competitiveness of American businesses. For example:

- Retail and hospitality establishments often offer Wi-Fi to customers, which may identify the physical location of the customers' devices as within range of the Wi-Fi signal. Such a service could easily connect with hundreds or thousands of customers each week.
- Retailers of all sizes maintain data about their customers' purchase history at their stores for loyalty and rewards programs. Such programs can include thousands of customers even for smaller retailers.
- Similarly, many retailers allow customers to create accounts with passwords and usernames and store data about charge cards to facilitate future transactions.
- Both U.S. businesses and the federal government have identified artificial intelligence (AI) systems as a key driver of economic growth and competitiveness. To perform tasks effectively and safely, many generative AI systems and foundation models are trained on large volumes of data on a broad variety of subjects.[12]

BRT recommends that the DOJ adopt bulk thresholds at least at the high ranges identified in the ANPRM.[13] If the DOJ, in its oversight of the proposed program over time, concludes that the bulk thresholds need to be adjusted lower to address national security risks, the DOJ should engage with industry to reassess an appropriate threshold.

III. Precision in Defining Geolocation Data [ANPRM Q10]

A wide variety of common applications such as ride-sharing services, delivery tracking and location-based advertising depend on geolocation information for functionality. BRT

[11] 89 Fed. Reg. 15788 (2024).

[12] See White House, Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, Section 3(k), Oct. 30, 2023, www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthydevelopment-and-use-of-artificial-intelligence.

[13] 89 Fed. Reg. 15786 (2024).

recommends that the DOJ's level of precision in defining geolocation should establish a radius equivalent to or greater than existing state laws. A uniform definition that restricts data showing location at a radius under 1,850 feet, as under California law,[14] would provide more consistency for compliance obligations associated with providing location-based services.

Consistent with our recommendation that the DOJ treat lower-risk information differently to ensure privacy while maintaining data utility, BRT recommends that the DOJ provide flexibility for industry "fuzzing" practices that reduce the precision of location data to a more general location. Geolocation information that has been made less precise than the established radius should no longer qualify as "precise geolocation information" under the program, provided that the fuzzing process cannot be reversed by a country of concern or covered person.

Finally, we seek clarity on proposed restrictions related to government-related data. The definition covers any precise geolocation data for any location enumerated on a list of government locations, regardless of volume.[15] In our view, restrictions on such data should apply only when companies are knowingly engaging in transactions to sell such data, consistent with other restricted data transactions.

IV. Business Use of Covered Sensitive Data in Cross-Border Context [ANPRM Q12]

The data covered under the ANPRM is used in a wide variety of contexts in global commerce, consistent with data protection laws. The DOJ should consider the following uses:

- Covered data is used to provide services directly, such as providing patient health care, financial risk assessment, or marketing or hospitality services to U.S. persons who are traveling abroad;
- Covered data may be stored in data centers physically located in multiple geographic regions to streamline cloud services, reduce latency and provide for business continuity during data security events;
- Covered data may be accessible to non-U.S. service providers performing administrative or operational functions, such as call center staffing;
- Covered data may be licensed or transferred as part of business-to-business transactions to U.S. companies operating abroad; and
- Covered data may be transferred as part of a required regulatory submission or through other legal processes to conduct business in countries of concern.

In these and other contexts, businesses strive to provide innovative services while using data responsibly and in compliance with privacy, security and consumer protection regulations. However, an overbroad approach to restricting commercial agreements, including low range

[14] Cal. Civ. Code section 1798.140(w).
[15] 89 Fed. Reg. 15787 (2024).

thresholds on bulk data, could impede uses of data that benefit Americans, create operational inefficiencies and disadvantage U.S. businesses in the global market.

As noted above, BRT recommends that the DOJ establish a framework that carefully considers business operations and routine data flows while mitigating the national security risks of countries of concern access to covered data. BRT supports the exemption of certain transactions proposed by the DOJ, including but not limited to personal communications, payment processing, compliance activities, intra-entity transactions incident to business operations, and transactions required or authorized by law.[16]

V. Enhancing Clarity in Definitions [ANPRM Q22]

BRT urges the DOJ to clarify the scope of restrictions on data brokerage and commercial agreements (i.e., vendor, employment and investment agreements), including clarification on the proposed definition of "covered data transaction." We note that "covered data transaction" as currently defined is broad and includes "any transaction that involves any bulk U.S. sensitive personal data or government-related data..."[17] We seek clarification on how "involves" should be interpreted.

Regarding commercial agreements, it is critical for the DOJ to clarify the role of countries of concern or covered persons in the definition. For example, the definition of vendor agreement applies to "any person" regardless of whether the person is a covered person or is located in a country of concern. However, the ANPRM's examples of vendor agreements each include a covered person or country of concern as party to the agreement, which seems in conflict with the ANPRM's restrictions on data brokerage.[18] If the DOJ's intention is to impose privacy and security safeguards on commercial agreements even in the absence of involvement by a country of concern or covered person, this would be a significant expansion of the scope of the ANPRM.

In addition, regarding commercial agreements, we seek clarification that such agreements are only covered when it involves sensitive personal data in bulk volumes. The DOJ should clarify that agreements involving data which do not meet the bulk threshold are out of scope.

Regarding the scope of covered and exempt commercial agreements, BRT appreciates the exemption of banking and payment services in Section H of the ANPRM and that this exemption 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, we request that the DOJ: (1) provide further clarity on the range of financial services within scope; and (2) confirm that specific operations

[16] 89 Fed. Reg. 15793-15795 (2024).
[17] 89 Fed. Reg. 15788 (2024).
[18] 89 Fed. Reg. 15788-15789 (2024).

related to payment processing are exempted, including the provision or processing of funds transfers and the provision of services ancillary to processing payments and funds transfers (e.g., payment dispute resolution, payor authentication, tokenization, payment fraud detection).

Regarding data brokerage, the definition proposed in the ANPRM is crafted in a manner that risks creating uncertainty and potentially covering a broader class of transactions than is intended.[19] This consequence arises from the open-ended nature of the term "similar commercial transactions," which, given its broadest possible reading, could include any data transfer of a commercial nature or any transfer relating to any commercial activity. The inclusion of three elements would help refine and clarify the definition: (1) a reference to data having to be sold, provided access to or otherwise transferred "for monetary or other valuable consideration;" (2) a knowledge standard (that data is knowingly collected and sold), in line with existing state law definitions;[20] and (3) a reference to the data itself having to be the object of the transaction, for example through clarification that data transferred in relation to the development, testing, production, distribution, or sale of a product or service is not considered "brokerage," where the data itself is not the product or service. These elements align with definitions of "data brokers" found in other contexts and are consistent with the policy objective set forth in Executive Order 14117 and the ANPRM.[21]

Regarding data brokerage, the DOJ should clarify that the ANPRM would exclude:

- Business-to-business transactions between U.S. companies where one U.S. company is located in a country of concern;
- Marketplace sales, in which a third-party seller that is located in a country of concern or that is a covered person provides items for sale to U.S. persons on platforms owned by U.S. companies;
- Retail advertising networks that are owned by U.S. companies and that feature advertisers who are covered persons or that are based in a country of concern;
- Personal health data and human genomic data for scientific research purposes;
- Personal data needed for the provision of telecommunications services; and
- Provisions of services to U.S. persons abroad.

Regarding investment agreements, we likewise ask for more clarity over the types of "indirect" ownership interests that would be covered and note concern about the breadth of this definition, together with the potential breadth of sensitive personal data. A broad definition of

[19] 89 Fed. Reg. 15788 (2024).
[20] See, e.g., Cal. Civ. Code 1798.99.80.
[21] See White House, Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, Feb. 28, 2024, https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern.

"investment agreement," even where covered persons are explicitly excluded from accessing sensitive personal data, could result in significant due diligence and compliance expense, including potential audit requirements, with respect to investments that do not pose a national security risk. For example, a regional retailer with bulk data on purchase history could be subject to the security requirements when taking an investment by a fund that is managed by a U.S. person general partner if a covered person has some influence on a limited partner advisory committee but no rights, influence or access with respect to the U.S. business itself. Similarly, an indirect investment by a covered person in a foreign parent company with such a subsidiary should pose little risk. We therefore propose that this definition be appropriately scoped, with the de minimis threshold set at a high level, and again recommend that the bulk thresholds be set at the upper ranges proposed by the DOJ to avoid discouraging benign investment flows.

VI. Ascertain Covered Persons in Data Transactions [ANPRM Q28]

The ANPRM seeks comment regarding the diligence necessary to ascertain whether a counterparty to the transaction is a covered person.[22] It can be challenging to ascertain with high confidence the ultimate ownership or control of modern corporate entities with complex, layered structures that span multiple jurisdictions. BRT suggests that the DOJ view the intensity of diligence necessary in terms of the degree of risk associated with a covered data transaction.

Transactions that are lower risk because of the data or parties involved should require less diligence, such as contractual representations or automated review of technical indicators (i.e., flagging or blocking IP addresses from certain regions). Higher risk transactions may require more diligence, such as manual review of public domain information about the counterparty, engaging with the counterparty's financial institutions or ensuring the counterparty is not present on restricted lists (such as sanctions lists or a DOJ-provided list of covered persons).

BRT recommends that the DOJ provide guidelines for businesses contrasting due diligence under the ANPRM with due diligence under sanctions and export compliance requirements. The DOJ should provide resources or tools to assist businesses, including small- and mid-sized enterprises, in conducting diligence to ascertain whether a counterparty is a covered person. This approach would allow for efficient allocation of resources while maintaining robust compliance standards.

VII. Considerations for Control by Countries of Concern [ANPRM Q29]

The ANPRM seeks comment on considerations regarding whether a person is "controlled by or subject to the jurisdiction or direction of" a country of concern for purposes of Attorney General designation as a "covered person."[23]

---

[22] 89 Fed. Reg. 15791 (2024).

[23] 89 Fed. Reg. 15790-15791 (2024).

BRT recommends the DOJ clarify how this language applies to an enterprise with its headquarters and primary place of business outside countries of concern but that maintains business operations in a country of concern. The DOJ should clarify that typical business operations within a country of concern are not covered by the regulations, such as selling products and services to residents of a country of concern, issuing equities on a stock exchange in a country of concern, or maintaining an office or agent in a country of concern. Components of the enterprise may be subject to the jurisdiction of the country of concern because of these business operations, but BRT believes it would be an overbroad interpretation for this alone to be the basis of a "covered person" designation.

BRT suggests the DOJ consider the proposed interpretive guidance of the Department of Energy (DOE) under the Infrastructure Investment and Jobs Act regarding "subject to the jurisdiction" of a covered nation.[24] The DOE's proposed guidance would clarify that an entity's activities outside the covered nation would not be designated a "foreign entity of concern," though an entity's activities inside the covered nation may be considered a "foreign entity of concern."[25]

VIII. Publishing the List of Covered Persons [ANPRM Q32]

BRT recommends that the DOJ publish a list of designated covered persons.[26] Obfuscating techniques, such as establishing multiple shell entities, can create challenges to ascertaining with high confidence that an entity is not a covered person. It would be more effective and less burdensome to enable U.S. persons to review a federally provided list of covered persons, rather than requiring U.S. persons to perform research independently.

Maintaining a public list of covered persons in similar formats to the Office of Foreign Assets Control (OFAC) sanctions lists would fulfill this function. This includes a search portal on a government-hosted site, human readable lists in PDF and text formats, and machine-readable lists in XML and CSV formats. The machine-readable list formats help to enable automated checks of counterparties against the list. Many companies presently use this technique for sanctions compliance, and BRT encourages the DOJ to leverage existing compliance efforts where possible.

IX. Industry Monitoring of the List [ANPRM Q33]

As with the OFAC Specially Designated National list, we recommend that the DOJ amend the program's public covered persons list to include aliases, pseudonyms and technical identifiers

[24] U.S. Department of Energy, Notification of Proposed Interpretive Rule Regarding Interpretation of Foreign Entity of Concern, 88 Fed. Reg. 84082 (2023), https://www.federalregister.gov/documents/2023/12/04/2023-26479/interpretation-of-foreign-entity-of-concern.
[25] 88 Fed. Reg. 84085-84086 (2023).
[26] 89 Fed. Reg. 15790-15791 (2024).

of covered persons as they become known.[27] While an automated notification system to alert registered users about updates to the list would assist businesses in staying current, continuous monitoring of the list would pose a substantially greater compliance cost than publishing updates at intervals. Given the dynamic nature of international relations and business activities, the list should be updated regularly. BRT suggests a regular schedule for list updates (e.g., quarterly) to better enable companies to coordinate compliance activities.

A challenge for the DOJ to consider is the expectation for businesses if an entity with which they have an established relationship is added to the covered persons list. If the relationship must immediately end, this could be disruptive. Announcing additions to the list in batch format at specific intervals, combined with an automated notification system, would help companies manage such circumstances.

X. Exemption of Intra-Entity Transactions [ANPRM Q43-44]

The conduct of business in today's global and highly digitalized economy entails frequent transfer of data—often across borders—among business units and affiliated entities. In certain cases, the structure of a corporate operation may result in such transfers being swept within the scope of covered transactions, despite such transfers not being the intended target of U.S. government regulation. The ANPRM recognizes this possibility and seeks to accommodate such transactions through an exemption, but the proposed language of the exemption creates confusion as to the scope of exempt transactions and risks diminishing the exemption's effectiveness.

The apparent dual-part test of transactions having to be both incident to business operations and part of ancillary operations raises questions regarding the kinds of transactions that may or may not be covered. The illustrative list of activities contained within the ANPRM is limited and does not account (indeed cannot account) for the range of possible intra-entity or routine transactions that could be implicated by the new rule. As such, we encourage the DOJ to revise its proposed approach to this exemption—which we strongly support—to provide that it will apply to transactions between a U.S. person and its subsidiaries or affiliated firms, where such transactions relate to the development, testing, production, distribution, or sale of the person's products or services or are necessary for the conduct of administrative corporate functions, provided that the data transaction is not itself the product or service being delivered.

To the extent that the rule scopes the intra-entity transaction exemption using the currently proposed language, we request further clarity on what is considered to be "ordinarily incident to and part of ancillary business operations."[28] For example, it would be of business interest in some cases for global companies to allow certain foreign persons with professional expertise to

[27] 89 Fed. Reg. 15791 (2024).
[28] 89 Fed. Reg. 15792, 15794 (2024).

access U.S. data (pending definitions) to perform a specific job function even though they are based in countries of concern.

We seek clarification on whether this is exempted, and if not, we welcome ways, such as adding security controls and standards, to ensure flexibility. If such uses are not exempted, it would in practice require all international U.S. persons with staff located in countries of concern to establish completely separate operational, technical, and communication systems enabling internal collaboration, customer management, contingency planning, and other routine business activities. It would also require the hiring of separate internal teams to provide all such support, including technical and other assistance.

Further examples of routine, low-risk transactions that should fall under this exemption include:

- Systems that enable routine communications across a group enterprise, including document management resources, email platforms, internal collaboration and review platforms, and video conferencing tools;
- Pricing systems and billing systems;
- Customer and vendor relationship management and onboarding and business contact registry; and
- Expense monitoring and reporting tools. Businesses with global operations may obtain travel expense monitoring and reporting tools and data-feeds from third parties (e.g. hotels, airlines, travel management companies) to manage their employees' expenses. Businesses may also obtain tools (and associated data) from third parties which help them manage their spend on suppliers.

These exemptions should cover both the service provider and the entity engaging the provider to support the core business function.

XI. DATA SECURITY REQUIREMENTS

While we understand that the Cybersecurity and Infrastructure Security Agency (CISA) is tasked with promulgating rules for data security requirements, we urge the DOJ to work with CISA and other agencies (including the Department of Homeland Security and the National Institute of Standards and Technology) to develop workable data security requirements for ensuring compliant data transfers under covered data transactions. Such requirements should be tailored to the risk profile of the data and the business and consistent with international standards. Poorly scoped or unworkable requirements would risk instituting a de facto data localization requirement for U.S. businesses.

* * *

BRT members have a strong commitment to collaborative solutions balancing national security, privacy and business innovation. We appreciate the DOJ's engagement with the private sector, as well as the affirmation of the President and the DOJ that the United States remains dedicated to protecting human rights while promoting cross-border data flows to enable international commerce.[29] BRT respectfully requests an opportunity to supplement these comments in a meeting with the DOJ as proposed in the ANPRM.[30] To that end, or if you have any questions regarding these comments, please contact Amy Shuart, Vice President, Technology & Innovation, at AShuart@brt.org.

[29] 89 Fed. Reg. 15782 (2024).
[30] 89 Fed. Reg. 15780 (2024).