Comments of the Software & Information Industry Association
Advanced Notice of Proposed Rulemaking on Sensitive Personal Data
Department of Justice, National Security Division
Submitted on April 19, 2024

The Software & Information Industry Association (SIIA) appreciates the opportunity to provide comments on the advanced notice of proposed rulemaking issued by the Department of Justice's National Security Division to implement provisions of Executive Order 14117, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" (the Order).[1]

SIIA is the principal trade association for those in the business of information, including its aggregation, dissemination, and productive use. Our members include nearly 400 companies reflecting the broad and diverse landscape of digital content providers and users in academic publishing, education technology, and financial information, along with creators of software and platforms used by millions worldwide, and companies specializing in data analytics and information services.

SIIA appreciates the Department's careful attention to how the personal data of Americans can be used to undermine U.S. national security. Our responses that follow are designed to help the Department to develop rules that will implement the objectives of the Order while avoiding new regulations that would impede U.S. businesses without mitigating the risk posed by bad actors or countries of concern. We recommend that the Department strive to align definitions with existing U.S. legal frameworks around privacy and sensitive data and exercise care with new "know your customer" rules that may create compliance burdens that outweigh the regulatory goals.

1. In what ways, if any, should the Department of Justice elaborate or amend the definition of *bulk U.S. sensitive personal data*? If the definition should be elaborated or amended, why?

We recommend that the Department align the definition of sensitive data with existing U.S. state comprehensive privacy laws. This would mean, among other things, excluding de-identified, pseudonymized, and encrypted data in alignment with existing law and with industry-standard encryption practices and guidance from the National Institute of Standards and Technology (NIST). Consistent with state privacy laws as well as the discussion draft of the American Privacy Rights Act, the Department should also carve out publicly available information. Restricting the transfer of information that is readily available to anyone would not further the national security purposes of the Order and would raise First Amendment concerns related to commercial publishing.[2]

2. Should the Department of Justice treat data that is anonymized, pseudonymized, de-identified, or encrypted differently? If so, why?

[1] National Security Division, Department of Justice, *Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern*, 89 Fed. Reg. 15780 (Mar. 5, 2024), available at https://www.govinfo.gov/content/pkg/FR-2024-03-05/pdf/2024-04594.pdf.
[2] *See Sorrell v. IMS Health, Inc.*, 564 U.S. 552 (2011).

At a high level, the use of specified anonymization techniques should be viewed as an exception to transfer thresholds as well as other prohibitions against transfers. Although anonymization, de-identification, pseudonymization and encryption are each executed and even defined differently under various state laws, if the techniques represent an effective shield against exploitation of personal data, then their use should exempt such data from restrictions that consequently do nothing to reduce risk.

Therefore, the Department should exempt from the scope of "sensitive personal data" and "government-related data" personal data that has been encrypted, anonymized or de-identified in such a way as to render it no longer "personal data" as defined under U.S. state comprehensive privacy laws. This ensures that understandings of personal data meet existing requirements and guidance under U.S. privacy law. It would also prevent adding to the complex federal *and* state patchwork of regulations and confusing consumers and compliance efforts by redefining "personal data."

Because the states employ different definitions for various anonymization practices, however, we would also encourage the Department to be clear about how it is using these terms. The terms "anonymized," "pseudonymized," and "de-identified" can be confusing because there is little agreement—among either technical and policy experts, legal practitioners, regulatory authorities, or state laws themselves—about how they should be used, and indeed which constitutes the highest level of anonymization. The Department will need to determine whether these categories should be defined according to their technicalities and process, or alternatively the level of risk they present.

Similarly, the terms "government-related data" and "bulk sensitive personal data" should explicitly exclude data when encrypted using industry-standard encryption, such as those which comply with cryptographic standards promulgated by the NIST. Encryption is commonly accepted as one of the most effective measures available to prevent third parties from accessing data without permission, and operates as a foundational security protocol for individuals, companies and governments around the world. In many state laws, it is also regarded as a *de facto* threshold for terms such as "anonymized," "pseudonymous" and "de-identified."

In fact, the Department's definition of "access" appears to acknowledge that the ability to decrypt may be fundamental to a third party's ability to access content. As such, encrypted data, where persons or countries of concern do not possess the key required to decrypt it, does not present the kinds of risks the Order and this rulemaking seek to address.

As with all technology, innovation presents new challenges and demands the development of new solutions. While work is ongoing to develop quantum computing capabilities that can decipher encrypted data, these efforts are far from a stage where they can be operationalized, let alone at the scale that would be required to decrypt the kinds of bulk data at issue in this rulemaking. Moreover, simultaneous work is underway to develop quantum resistant cryptographic algorithms, of which NIST has approved several.

Given the significant work already being undertaken in this space, most encryption experts and researchers from academia, private and public sectors, and the open-source community expect that modern encryption schemes will continue to advance ahead of increases in scalable computational technology (including the availability of quantum computing at scale).

Including encrypted data in the scope of this rulemaking by defining it as "sensitive personal data" would also set a concerning precedent about the treatment and security presumptions of encrypted data, while failing to further the stated purpose of the Order. It would also run counter to the Order's instruction that the Attorney General "carefully calibrate[] actions to minimize the risks associated with … disruption to commercial activity."[3]

3. Should the Department of Justice consider amending the definitions applicable to any of the six categories of *sensitive personal data*? If the definition should be elaborated or amended, why?

As the Department recognizes, specific categories that are narrowly tailored to protect against harms derived from the highest risk uses of data are critical. Regarding "biometric identifiers," the Department is also correct to recognize that data about an individual's physical characteristics poses risks when it still may be used to recognize or verify their identities. We also appreciate the Department's grounding of "personal health data" in HIPAA and its implementing regulations, which helps to facilitate compliance.

The Department may consider clarifying the definition of "covered personal identifiers." We appreciate the Department's recognition that, as described in the Order, there are two important limitations on the scope of this category. First, under the Order, covered personal identifiers must be "personally identifiable data." Second, they must, perhaps when combined with other data, be made "exploitable by a country of concern." However, as currently defined, "covered personal identifiers" could encompass some combinations of listed identifiers that are neither personally identifiable data nor exploitable by a country of concern. To address this inconsistency, we would suggest that the Department draft proposed final rules to specify how it would resolve this inconsistency.

Specifically, we recommend the Department (1) state explicitly that data do not constitute "covered personal identifiers" if the data—even if it is a combination of linked listed identifiers—would be considered de-identified data outside the scope of state-level comprehensive privacy laws in the United States; and (2) when drafting proposed final rules, further refine what particular risks must arise for "covered personal identifiers" to be "exploitable by a country of concern."

4. Are there categories of *bulk U.S. sensitive personal data* that should be added to the definition? Are there categories proposed that should be removed? Please explain.

The Department should consider removing "covered personal identifiers" as a standalone category of "sensitive personal data" because it captures identifiers that U.S. state-level comprehensive privacy laws do not consider to be sensitive on their own. Instead, the Department should only consider "covered personal identifiers" to be sensitive when they are combined with any of the other categories of "sensitive personal data" in the Order.

7. What thresholds for datasets should apply with respect to each category of *bulk U.S. sensitive personal data* under consideration, and why is each such threshold appropriate? Should any category of *sensitive personal data* (*e.g., covered personal identifiers*) have different thresholds for different subtypes or specific fields of data based on sensitivity, purpose, correlation, or other factors?

[3] *Id.* at 15423.

We do not see a specific issue with the thresholds as set out. Setting out specific provisions for when a threshold may be deviated from due to increased or decreased risk could enable for a more fluid approach that best reflects the actual risk inherent to a specific set of information.

8. Are there other factors or characteristics that the Department of Justice should evaluate as part of the proposed analytical framework for determining the bulk thresholds?
9. What data points, specific use cases, or other information should the Department of Justice consider in determining the bulk thresholds for *bulk U.S. sensitive personal data*?

We strongly recommend that the Department exclude publicly available information from the definition of "sensitive personal data." Including publicly available information in the definition raises constitutional concerns and would impose a burden on firms that would be unlikely to advance the national security or personal privacy objectives of the Order. This is in part because this category of data is freely available to parties outside of the United States. Restrictions placed upon publicly available information are also unlikely to achieve any meaningful impact upon bulk data brokering to countries of concern because the market for such data is at least in part outside the jurisdiction of the United States. In fact, there is a real chance of fostering a secondary market for such data over which the United States would lack sufficient influence to protect its interests. U.S. actors would in turn be subject to limitations that do not reasonably advance national security interests.

Providing a clear and appropriately limited definition of "publicly available information" would be helpful. We recommend the Department rely on well-established definitions that have become a bedrock in the U.S. data protection framework. In particular, state comprehensive privacy laws exclude publicly available information. These laws define "publicly available data" to mean information made lawfully available to the public either by the individual or through government record, media outlet, or a third-party disclosure.[4] Each state's privacy law also provides that "publicly available data" is exempted from the category of "personal data," in part due to First Amendment considerations. The Department should explicitly exempt such data from the scope of "sensitive personal data" and "government-related data". Not only would this ensure alignment with existing laws, but it would also ensure that the final rules are properly targeted to realistic risks.

The Department may also consider removing "covered personal identifiers" as a standalone category of "sensitive personal data" because it captures identifiers that U.S. state-level comprehensive privacy laws do not consider to be sensitive on their own. Instead, the Department should only consider "covered personal identifiers" to be sensitive when they are combined with any of the other categories of "sensitive personal data" in the Order.

10. At what level should the Department of Justice set the precision (*i.e.,* numbers of meters/feet) in defining *precise geolocation data*? What are common commercial applications of geolocation data, and what level of precision is required to support those applications? When geolocation data is "fuzzed" in some commercial applications to reduce potential privacy impacts, what are common techniques for "fuzzing" the data, what is the resulting reduction in the level of precision, and how effective are those techniques in reducing the sensitivity of the data? To what extent should the definition be informed by the level of precision for geolocation data used in certain state data-privacy laws, such as a radius of 1,850 feet (*see, e.g.,* Cal. Civ. Code section 1798.140(w)) or a radius of 1,750 feet (*see, e.g.,* Utah Civ. Code section 13–61–101(33(a)))?

[4] *See* Cal. Civ. Code § 1798.192 (2022).

We believe the Department should define precise geolocation data such that it is aligned with the U.S. state privacy laws. For example, the California Privacy Rights Act (CPRA) defines precise geolocation data as: "*any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet."* This ensures that understandings of "precise geolocation data" within the Order aligns with common understandings in U.S. law and avoids muddying the waters and creating a definitional patchwork.

11. Should the Department of Justice consider changing any of the categorical exclusions to the definition of *sensitive personal data*? How should the program define the exclusion for data that is lawfully a matter of public record, particularly in light of data that is scraped from the internet or data points that are themselves public but whose linkage to the same individual is not public? What types of data are generally available to the public through open-access repositories?

The Department should consider clarifying the exclusion of public data in two ways. First, for the purpose of aligning with existing privacy laws, we would encourage the Department to rely on the definition of "publicly available information" from the Virginia Consumer Data Privacy Act (VCDPA). This is defined as "information that is lawfully made available through federal, state, or local government records, or information that [the disclosing party] has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by [the identifiable U.S. individual to whom the information relates], or by a person to whom [the identifiable U.S. individual] has disclosed the information, unless [the identifiable U.S. individual] has restricted the information to a specific audience."[5]

With regard to the Department's concern about public data that becomes linked to an individual through the use of non-public data, we would encourage the Department to anchor its analysis in the foreseeability of this linkage by the disclosing transacting party. Only if that linkage is reasonably foreseeable by the disclosing transacting party should the data be "sensitive personal data," assuming it meets the other conditions for falling into one of the six categories of sensitive personal data. This is because without this clarification, nearly any public data point could be said to be "sensitive personal data." It is at least theoretically possible that any receiving transacting party could find some way of linking any public data point to an individual using any theoretical non-public data points.

Further, the Department should broaden the financial services exception to encompass general compliance with US law. Carve-outs to the exception for national security reasons should be made on a case-by-case basis but obligations arising under legal compliance (i.e. for FCRA or GLBA compliance) should be acceptable as the default position.

We understand the Department is not considering the linkage of publicly available data being transferred by otherwise unaffiliated parties. For example, Entity A would have the ability to link data sourced separately from Supplier A and Supplier B. However, Entity B might not have the same freedom to link data sets sourced from its affiliates. The effect of this is to penalize parties who seek to transfer public data sets which could be linked to other data sets under their control. Such an approach would not further the goals and purpose of the Order and would only serve to penalize intra-company transactions. The default position should be that public information is inherently transferable without restriction.

[5] Code of Virginia Code - Chapter 53. Consumer Data Protection Act.

14. With respect to defining *linked* for purposes of *covered personal identifiers,* should the Department of Justice consider placing a time limit on when *listed identifiers* would be considered *linked* to address a scenario in which, for example, a *U.S. person* sells a bulk list of names to a *covered person* on day one (which would not be a *covered data transaction*) and then sells a list of Social Security Numbers associated with those names years later? Would the lack of such a time limit require or encourage U.S. companies, such as data brokers, to retain *sensitive personal data* that they would otherwise purge in the normal course of business?

Data retention practices are likely already in place for most of these data sets. However, and depending upon the exact calculation of time, new retention schedules may actually result in a requirement that firms retain data longer than would otherwise be necessary and conflict with existing law and practice. To the extent that a time limit is imposed, it should be commensurate with existing data retention practices for the data sets at issue.

15. With respect to defining the term *covered personal identifiers,* how should the Department define the subcategory of listed classes of personally identifiable data "in combination . . . with other data that is disclosed by a transacting party pursuant to the transaction that makes the personally identifiable data exploitable by a country of concern"?

We recommend that the Department limit this definition to data sets disclosed by a single party or group of affiliate parties. Without this restriction, data sets disclosed by multiple transacting parties could be read to render the personally identifiable data exploitable "in combination … with other data that is disclosed by a transacting party."[6] This should not be broadened further, lest U.S. entities inherit uncontrollable risk. This includes risk derived from linkable data sets controlled by entirely unaffiliated parties.

16. How should the Department define *information or informational materials*? What factors should the Department take into account in its definition? What relevant precedents from other IEEPA-based programs should the Department take into account when defining the term?

We suggest that the Department clarify that the rules are not intended to regulate any internet traffic, including both content and metadata, transiting to end-users in countries of concern where that data is created or transmitted by or on internet-based platforms or services that are designed to create or exchange any content that is expressive in nature. U.S. companies or persons consistently send information, including covered information, on internet platforms that is intended for further distribution to other users of the Internet – including to individuals and companies in countries of concern.

This interpretation would align with Congress' intent when it enacted and updated the IEEPA Berman Amendment to "facilitat[e] transactions and activities incident to the flow of informational materials…to ensure the robust exchange of informational materials."[7] Such data is necessarily personal communications, information, or informational materials excluded from the Executive's authority under 50 U.S.C. 1702(b)(1) & (3).

---

[6] National Security Division, Department of Justice, *Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern*, 89 Fed. Reg. 15787 (Mar. 5, 2024), available at https://www.govinfo.gov/content/pkg/FR-2024-03-05/pdf/2024-04594.pdf.

[7] *United States v. Amirnazmi*, 645 F.3d at 586, 587.

17. In what ways, if any, should the Department of Justice elaborate or amend the definition of government-related data, including with respect to "recent former" employees or contractors, and "former senior officials"?

We believe the Department should provide clear, bright line rules clarifying when an individual constitutes a "recent former" employee or contractor as well as "former senior official." This will ensure these requirements are consistently interpreted and operationalized across industry.

22. What modifications to enhance clarity, if any, should be made to the definitions under consideration for *data brokerage, vendor agreements, employment agreements,* and *investment agreements* ?

We strongly urge the Department to define "data brokerage" in alignment with existing state laws. For example, California defines the term as follows:

"Data broker" means a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship. "Data broker" does not include any of the following:

(1) An entity to the extent that it is covered by the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.).

(2) An entity to the extent that it is covered by the Gramm-Leach-Bliley Act (Public Law 106-102) and implementing regulations.

(3) An entity to the extent that it is covered by the Insurance Information and Privacy Protection Act (Article 6.6 (commencing with Section 791) of Chapter 1 of Part 2 of Division 1 of the Insurance Code).[8]

We also believe the circumstances under which a vendor or employment agreement "involves" covered data should be more fully defined. While the ANPRM lays out a handful of specific examples, no definition of "involves" is provided, and the examples given are not sufficient for U.S. companies to identify the full range of covered agreements. To resolve this problem, we suggest that the Department define what it means to "involve" covered data or, alternatively, specify that only vendor or employment agreements where access to data is contemplated as part of the vendor's or employee's responsibilities then "involve" covered data and are subject to the new rules.

Further, the Department should exempt from the scope of vendor agreements those in which: 1) the vendor is providing product research, development, or improvement services for a U.S. person, 2) any sensitive personal data is processed by the vendor only in ways ordinarily incident to and part of that product research, development, or improvement, 3) the U.S. person directs and controls the manner of processing the data, and 4) the vendor is contractually bound by the U.S. person to maintain the privacy and security of the data. This is because many U.S. companies rely on suppliers and manufacturers in other countries to produce and assemble products. When such physical products involve data processing, providing those suppliers and manufacturers with data is often necessary to enable product development, testing, and quality control. Assuming that covered entities carefully control their vendors' processing of this data, such arrangements should not fall within the scope of vendor agreements.

[8] California Civ. Code 1798.99.80.

We lastly suggest that the definition of employment agreement, and others, should be modified to more closely incorporate the definition of covered individuals. For example, the definition should clarify when the counterparty to a contract is properly considered a covered individual relevant and when it is not. Contracting parties should also be able to rely primarily upon official designation by the Department and then, secondarily, upon specifically delineated due diligence factors that are reasonable under the specific circumstances of the contract at issue.

24. Are there any elements of the *data brokerage* ecosystem that would not be included in the definition of *data brokerage* under consideration?

The definition of "data brokerage" must exclude publicly available information, as well as service providers. As discussed above, publicly available information is constitutionally protected by the First Amendment, yet covering this information under the definition of "data brokerage" would lead to its restriction under the Order and thus fail to meet constitutional muster.

Service providers, or entities that process covered data on behalf of covered entities, should also be exempt from this definition. If they are not exempt, transfers of data to service providers, whose processing is often necessary for routine business purposes, would be restricted as data brokerage. Service providers do not implicate the same concerns as other data recipients, since the data received is merely processed on behalf of the covered entity. It is not retained, passed onto third parties, or combined with other covered data being processed by the service provider.

28. How would the U.S. party to a data *transaction* ascertain whether a counterparty to the transaction is a *covered person* as defined above? What kind of diligence would be necessary?

The level of diligence should be encompassed by a background check akin to Foreign Corrupt Practices Act (FCPA), know-your-customer (KYC), and similar assessments. This would establish a threshold of demonstrable compliance. However, this is a challenging tightrope act for compliance departments. Foreign governments, especially those listed as countries of concern, are often not willing participants in data sharing with U.S. companies attempting to ascertain whether a counterparty located within their jurisdiction is a covered person as defined. Even domestically, recent restrictions placed on risk data providers who process data—such as Beneficial Ownership Information (BOI) on behalf of U.S. companies that aided in these assessments—have curtailed visibility by U.S. corporate compliance teams. Therefore, primary responsibility for designation of a counterparty as a covered person should still rest with the Department.

29. What are the considerations as to whether a *person* is "controlled by[] or subject to the jurisdiction or direction of" a *country of concern* ? What, if any, changes should be made to the definitions above to make their scope and application clearer? Why? What, if any changes should be made to broaden or narrow them? Why?

Unless there has been a specific finding that a specific country of concern poses such an inherent risk to national security concerns, mere residence within a country should not be sufficient to automatically establish that an individual is a covered person. While considerations of "control" may be similar to those employed in KYC or FCPA compliance – they may not be sufficiently similar that private actors would be adequately experienced to make the necessary national security assessment without further guidance. Moreover, establishing a KYC regime for data transfers without the underlying domestic and international legal framework that is a foundation for KYC in the financial services space cannot

prevent bad actors from undertaking efforts (such as incorporation in a third country or use of intermediaries) to evade transfer restrictions. We suggest that good faith due diligence should be supplemented by official guidance and designations by the Department.

30. With respect to the part of the definition of *covered person* addressing "a foreign person who is primarily resident in the territorial jurisdiction of a *country of concern,*" how should the Department of Justice address temporary travel to or in a *country of concern* by foreign individuals who are not citizens of a *country of concern*? Should the standard be "primarily resident in," "resident in," "located in," or something else?

We believe blanket restrictions based solely upon residence or travel are problematic and should not be a primary factor in identifying which individuals are covered persons. Similarly, the burden of identification should not be placed upon private parties, who are not generally suited to assessing whether temporary travel or primary residence in a specific instance is problematic from a national security standpoint. With that in mind, we suggest a tiered approach where the Department is empowered to designate specific individuals as covered persons as a first-tier compliance requirement. The Department could then issue general directives and guidelines regarding residency, and temporary travel could be viewed as sufficient grounds to label a party as a covered person. This would place covered entities on notice that they are at a higher level of risk of dealing with a covered person and must act appropriately while engaging with that individual.

33. How would industry monitor this list? Would it be more costly for industry if the list were updated continually or only at certain points in time? If updates were made on an individual basis or in batches? Please be specific.

It would be significantly more expensive for businesses if the list were 1) constantly updated, or 2) updated on an individual basis. This would impose a burden on businesses to maintain moment-to-moment awareness and implementation of any lists' contents and updates. However, it is possible that risk data providers could be leveraged to provide services for businesses seeking to monitor this list. This would be similar to how FinCEN currently operates, where third party businesses consult with risk data providers regarding updates and analysis of the databases it maintains.

39. How feasible is it to contract with prospective customers to prevent pass-through sales, re-sale, or onward transfers of *bulk U.S. sensitive personal data* or *government-related data* to *countries of concern* or *covered persons*? Do technical means exist to prevent such onward sales or transfers? If yes, what are such technical means?

These goals are typically accomplished through contractual terms in a data privacy context, so it should be feasible to introduce additional contract terms to achieve the same ends. However, contractual terms will not ensure that onward transfer of data does not occur. Indeed, it is virtually impossible to prevent this from occurring, and beyond the scope of any private entity to ensure compliance and monitor what happens with data after a transaction occurs.

In addition, we believe the Department should exempt contractual agreements governing the exchange of internet traffic with foreign carriers from rulemaking related to "vendor agreements." These include rulemaking intended to prevent pass-through sales, re-sale, or onward transfers.

41. What, if any, unintended consequences could result from the proposed definitions?

We are particularly concerned that these definitions could create a "chain of accountability" scenario as data is used downstream. We suggest considering a scenario where a U.S. entity sells a data set to a third party. This third party has an office with employees in a country of concern, which has both American employees and employees with ties to the foreign government. A U.S. company sells to this third party's U.S. office and that third party permits that data to be accessed by the foreign office – and therefore the employees and government of this country of concern. In this case, does the U.S. company need to confirm who each of their purchasers' employees are in each of their foreign offices to avoid liability? Is this U.S. business required to implement initial safeguards necessary to block these employee's access?

A related, but separate, concern is also the list of entities whose association with a country of concern restricts them from receiving data from U.S. companies. This is especially salient for entities on the list that are owned by a country of concern or an entity located in those countries. While there may be ways to determine how not to do business with a company located in a country of concern, the question of ownership is nearly impossible for companies to determine.

43. Are there other types of data transactions that should be exempt? Please explain why.

We suggest that data transactions covered under the Fair Credit Reporting Act (FCRA) and those related to risk intelligence-related services should be exempted. This is because these services are designed to enable parties to identify and remediate precisely those situations where countries of concern could exploit data subjects. Restricting such transfers would hamper the ability of parties to protect themselves against the very risks the Order is intended to prevent. Conversely, this data is not particularly useful for the type of exploitation that motivates the restrictions imposed by the Order.

57. Would an advisory opinion process in general be useful? What effect, if any, should the issuance of an advisory opinion have for the party or parties who requested it? For third parties?

The Order is based on national security concerns but addresses areas of law and practice that are typically commercial in nature. The different approach makes advisory opinions particularly valuable to commercial actors who may lack sufficient expertise to independently assess the national security concerns underlying the Order. Reliance upon an advisory opinion, even by third parties, should constitute demonstrable compliance with the requirements of the Order and related Rules.

58. Should industry groups or other associations be permitted to request advisory opinions or interpretive guidance on behalf of one or more of their members (noting that such requests would still need to identify all relevant participants in a data *transaction*)?
59. Should some or all advisory opinions be published? How might the possibility of publication affect a request (noting that any publication would comply with applicable laws regarding confidential business information and similar topics)?

We believe advisory opinions are necessary here for two reasons. First, because private actors are unlikely to have a strong appreciation for the national security concerns at issue, the ability to obtain advisory opinions would be extremely helpful. Second, advisory opinions aid compliance departments in making decisions aided with the knowledge that they will not run afoul of the transfer restrictions. This avoids chilling those transfers that would potentially be productive, but are nevertheless avoided due to a potentially faulty understanding of the restrictions or national security priorities.

For this reason, we also believe these advisory opinions should be published for future reference by other U.S. companies. Publication will avoid the need for constant requests in similar contexts and similarly aid compliance departments in ascertaining the legality of a transfer. It will also prevent additional requests for otherwise redundant advisory opinions from consuming Department resources.

64. What types of information would be useful to include in the know-your customer and know-your-vendor due diligence described above? Do customers and vendors generally have this information readily available?

To comply with the Order, it would be critical to be able to assess the degree of connection between a vendor or customer and either a country of concern or a covered individual. Some of this information, such as residence or country of incorporation, may be on hand. However, the extent to which specific sets of information are indicia of control or influence by a country of concern or covered individual may not be readily apparent. They may also be substantially different than metrics used in either KYC or FCPA analysis.