February 29, 2024

Invoking National Security Risks, President Biden Issues Executive Order Restricting the Transfer of Certain Sensitive U.S. Personal Data to Countries of Concern

On February 28, President Biden issued Executive Order 14117 on "Preventing Access to Americans' Bulk Sensitive Data and United States Government-Related Data by Countries of Concern"[1] (the "Order").

The Order establishes that it is the policy of the United States to "restrict access by countries of concern to Americans' bulk sensitive personal data and United States Government-related data when such access would pose an unacceptable risk to the national security of the United States" and directs certain agencies to take actions in furtherance of that objective.[2]

The Order directs the Department of Justice ("DOJ") to issue regulations to implement its central objectives. DOJ released an Advanced Notice of Proposed Rulemaking ("ANPRM") that proposes the framework for such a rule, which is described in greater detail below.[3]

Generally, the ANPRM contemplates a regulatory regime where data transactions involving bulk sensitive U.S. personal data would be prohibited or restricted when they involve specified Countries of Concern—China, Russia, Iran, North Korea, Cuba and Venezuela—or covered persons subject to their jurisdiction ("Covered Persons"). The regulation would broadly define sensitive U.S. personal data, including a wide array of personal identifiers linked to U.S. persons digital identity (*e.g.*, cookies, IP addresses, call-detail data, social security numbers, SIM card numbers, etc.).

The Order would broadly *prohibit* data transactions that involve a U.S. person providing bulk sensitive U.S. personal data to covered persons, whether through a sale or providing access through a license or subscriptive service. The Order would also apply *restrictions* on U.S. companies' vendor agreements, employment agreements and investment agreements that would provide a Covered Person with some access to covered data. For restricted transactions, the companies will need to comply with certain "security requirements" that the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA") will issue.

---

1 The White House, *Executive Order 14117 on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern* (Feb. 28, 2024), available here.

2 Order § 1.

3 ANPRM on Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern, Docket No. NSD 104, available here.

This is a significant regulatory development for companies that hold sensitive U.S. personal data. While the Order does not take effect immediately, it does signal that this is an area of significant regulatory scrutiny. The selection of DOJ as the lead agency to implement these regulations also suggests that there will be a significant emphasis on enforcement.

Background

The Order attempts to fill what the Department of Justice described as "a key gap in our national security authorities" by providing DOJ "a new and powerful enforcement tool to protect Americans and their most sensitive information from being exploited by our adversaries."[4]

U.S. national security officials have in recent years become increasingly concerned about the risks related to the sale of sensitive personal information to foreign actors and, in particular, about the role of "data brokers" in this market; the federal government's authorities in this area have been fairly limited.[5] This concern has been underscored by media reports about how sensitive data sets on military personnel, including information about health conditions and financial metrics, could be readily and legally purchased at a low price from data brokers and other intermediaries.[6] A 2018 *Washington Post* study noted that a fitness company that published a map based on users' geolocation data established, in effect, the outlines of U.S. military bases, which could raise operational security issues.[7]

Given the growing concerns about foreign actors' access to sensitive U.S. data, in 2018 Congress passed legislation that, in relevant part, expanded CFIUS's[8] authority to review non-passive, non-controlling investments in U.S. businesses that hold sensitive personal data of "United States citizens that may be exploited in a manner that threatens national security."[9] To underscore that sensitive personal data are a significant concern for CFIUS, President Biden's September 2022 Executive Order (14083) explicitly identified sensitive personal data as one of the central issues that CFIUS should review in a transaction and noted that information relating to health, digital identity or other biological data of U.S. persons is particularly sensitive.[10]

However, CFIUS's jurisdiction only extended to foreign *investments* in U.S. businesses—it did not extend to the sale or transfer of sensitive personal data to foreign actors, including in countries of concern. DOJ notes that "no existing laws comprehensively and prospectively address the national security risks posed by access by countries of concern or covered persons subject to their

---

4 Department of Justice, Office of Public Affairs, *Justice Department to Implement Groundbreaking Executive Order Addressing National Security Risks and Data Security* (Feb. 28, 2024), available here.

5 Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Feb. 6, 2023), available here.

6 Tonya Riley, *Brokers Sell Military Members' Data for Pennies, Study Finds*, Bloomberg Law (Nov. 6, 2023), available here.

7 Liz Sly, *U.S. Soldiers Are Revealing Sensitive and Dangerous Information by Jogging*, Washington Post (Jan. 29, 2018), available here.

8 CFIUS is the acronym colloquially used for the interagency Committee on Foreign Investment in the United States.

9 *See* Foreign Investment Risk Review Modernization Act of 2018. In January 2020, the Treasury Department released final regulations implementing that legislation. *See* Paul, Weiss, *Final CFIUS Regulations Implementing the Foreign Investment Risk Review Modernization Act of 2018 Are Now in Effect* (Feb. 27, 2020), available here. Under those regulations, investment implicating sensitive personal data are subject to mandatory CFIUS review if (1) the U.S. business (a) targets or tailors products or services to certain populations (e.g., the U.S. military or federal employees), (b) collects or maintains such data on at least one million individuals, or (c) has a business objective to collect or maintain such data on greater than one million individuals and such data are an integral part of the business's products or services; and (2) such identifiable data fall within any of 10 categories, including certain types of financial, health, non-public electronic communication, geolocation and biometric data. *See* 31 C.F.R. § 800.241.

10 The White House, *Executive Order on Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States* (Sep. 15, 2022), available here.

jurisdiction or control to sensitive personal data through commercial transactions. This targeted new program will be designed to address this gap in U.S. national security authorities."[11]

The Executive Order

The Order is issued pursuant to the President's authority under the International Emergency Economic Powers Act ("IEEPA"). Though the President has historically utilized this authority to declare "national emergencies" for purposes of establishing country-based or activity-based sanctions programs (such as regarding Russia, Iran or North Korea or weapons proliferation or transactional criminal organizations), it has been increasingly utilized by recent presidents, such as President Trump and President Biden, as a mechanism to declare or further "national emergencies" to establish broad-based regulatory regimes, such as in the 2022 "outbound investment" Executive Order.[12]

The Order does not have any immediate effects but instructs various agencies to take relevant actions:

- *DOJ*: Within 180 days of the Order, DOJ shall publish a proposed rule that defines the categories of prohibited transactions and restricted transactions.[13] The Order also makes DOJ responsible for issuing "licenses" authorizing transactions that are otherwise prohibited or restricted.[14]

- *CISA*: CISA shall publish the "security requirements" that address the "unacceptable risk" posed by the restricted transactions identified by DOJ. The Order specifies that the requirements "shall be based on the Cybersecurity and Privacy Frameworks developed by the National Institute of Standards and Technology."[15]

- *Team Telecom*: The Order notes that the "risk of access to this data by countries of concern can be, and sometime is, exacerbated" where the data transits a submarine cable that is linked to a Country of Concern and instructs Team Telecom to take measures to address this risk under its licensing program.[16]

- *Federal Participants in the Healthcare Market*: The Order notes the particular risks arising from access to "bulk sensitive personal data" in the healthcare market including "personal health data and human genomic data" which can be obtained "through partnerships and agreements with United States healthcare providers and research institutions."[17] To address this risk, the Order instructs the Department of Defense, The Department of Health and Human Services, the Department of Veterans Affairs and the National Science Foundation to consider taking steps to "prohibit the provision of [federal] assistance that enables access by countries of concern or covered persons to United States persons' bulk sensitive personal data" or would impose appropriate "mitigation measures" on such access consistent with the "security requirements" established by CISA.[18]

---

11 Department of Justice, *FACT SHEET: Justice Department Will Issue Advance Notice of Proposed Rulemaking Following Forthcoming Groundbreaking Executive Order Addressing Access to Americans' Bulk Sensitive Personal Data by Countries of Concern* ("Fact Sheet"), available here.

12 Paul, Weiss, Economic Sanctions and Anti-Money Laundering Developments: 2023 Year in Review (Jan. 22, 2024), available here.

13 Order § 2(c)(i)-(ii).

14 Order § 2(c)(v).

15 Order § 2(d).

16 Order § 3(a). Team Telecom is shorthand for the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector.

17 Order § 3(b).

18 Order § 3(b).

- *CFPB*: The Order notes the particular risks arising from the "data brokerage industry" and "encourages" the Consumer Financial Protection Bureau to take steps to "address this aspect of the threat," including through additional rulemakings.[19]

The DOJ's Advanced Notice of Proposed Rulemaking (ANPRM)

DOJ stated that it is seeking to "establish generally applicable and transparent rules for engaging in specific categories of data transactions with certain countries of concern or covered persons subject to their jurisdiction."[20] In the ANPRM, DOJ provides a framework for many of the critical areas of a rule.

1. Covered Persons

As noted, the ANPRM contemplates identifying China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba and Venezuela as Countries of Concern. The regulation will also restrict U.S. persons' data transactions with "covered persons," which are defined in the Order to include:

(a) "an entity owned by, controlled by, or subject to the jurisdiction or direction of a country of concern" (note that the ANPRM applies this by including in its definition of "covered person" any entity that is "organized or chartered under the laws of, or has its principal place of business in, a country of concern," as well as "any entity that is 50 percent or more owned, directly or indirectly," by any covered person);[21]

(b) "a foreign person who is an employee or contractor of such an entity";

(c) "a foreign person who is an employee or contractor of a country of concern"; and

(d) "a foreign person who is primarily resident in the territorial jurisdiction of a country of concern."[22]

The Order also authorizes DOJ to "designate[]" specific persons as Covered Persons based on specified criteria.[23] DOJ noted that it intends to "publish and regularly update this non-exhaustive list of designated covered persons[.]"[24]

DOJ contemplates that a "foreign person" would *exclude* any "U.S. person." This means that any U.S. citizen, national or lawful permanent resident as well as any entity "organized solely under the laws of the United States" as well as any "foreign branches," or any person in the United States would not be a "foreign person" under the rule.[25]

Notably, as contemplated in the ANPRM, the definition of Covered Persons would not be limited to persons who are physically present in a Country of Concern. For example, a foreign company that is "controlled by" or subject to the jurisdiction or direction of a Country of Concern would be a Covered Person. Furthermore, the employees and contractors of an entity owned by,

---

19 Order § 3(c).

20 Fact Sheet at 2.

21 ANPRM at 42. This suggests, for example, that a majority-owned U.S. subsidiary of China-headquartered company is a "covered person." The other materials released by DOJ, however, suggest some potential ambiguity on this point. *See* Fact Sheet at 2 (stating that "anyone who is a U.S. citizen, national, or lawful permanent resident . . . and any entity organized solely under U.S. laws or jurisdiction; and any person located in the United States would not fall in these categories of covered persons."

22 Order § 7(d).

23 Order § 7(d) (DOJ can designate a person as a "covered person" based on their "being owned or controlled by or subject to the jurisdiction or direction of a country of concern, as acting on behalf of or purporting to act on behalf of a country of concern or other covered person, or as knowingly causing or directing, directly or indirectly, a violation of this order or any regulations implementing this order").

24 Fact Sheet at 2.

25 ANPRM at 33-34.

controlled by, or subject to the jurisdiction or direction of a country of concern would be considered Covered Persons, even if they are not located in a Country of Concern.

2. Bulk Sensitive Personal Data

(a) Sensitive Personal Data

The Order defines sensitive personal data as "covered personal identifiers, geolocation and related sensor data, biometric identifiers, human 'omic data, personal health data, personal financial data, or any combination thereof . . . and that could be exploited by a country of concern to harm United States national security if that data is linked or linkable to any identifiable United States individual or to a discrete and identifiable group of United States individuals."[26] DOJ is directed to "further define[]" these categories in its regulations.

The ANPRM provides further definition on these categories. The ANPRM contemplates including the following as sensitive personal data[27]:

(i) Covered personal identifiers: The ANPRM contemplates publishing a broad list of "listed identifiers" determined by the regulations to be "reasonably linked to an individual" under the definition of "covered personal identifiers". This would include government IDs or account numbers (such as a Social Security number); financial account numbers (such as associated with a financial institution); device-based or hardware-based identifiers (such as a SIM card number); demographic or contact data (such as name, DOB, address, phone number and email); advertising identifiers; account authentication data (such as account username, password or answer to a security question); network-based identifiers (such as IP address or cookie data); or call-detail data.[28] A "covered personal identifier" would include where "any listed identifier that is linked to any other listed identifier," with certain exceptions (where demographic or contact data is linked to other demographic or contact data).[29] This means that the transfer of "two listed identifiers" in a way that linked them, such as "in a single spreadsheet," would be sensitive U.S. personal data. For example, the transfer of "mobile advertising IDs linked to email addresses" would be considered sensitive personal data.[30] The ANPRM also contemplates that DOJ will issue additional guidance on covered personal identifiers on other subcategories of this definition, such as where particular data could be "exploitable by a country of concern." As examples, the ANPRM notes that the sale of a list of "active-duty LGBTQ+ military officers" even without other identifiers would be prohibited.[31]

(ii) Precise geolocation data: The ANPRM contemplates only regulating "geolocation and related sensor data" insofar as it relates to "precise geolocation data."[32] The ANPRM defines this as "data, whether real-time or historical, that identifies the physical location of an individual or a device with a precision of within [*number of meters/feet*] based on electronic signals or inertial sensing units."[33] The ANPRM solicits public comment on the precise distance that

26 Order § 7(e).

27 Fact Sheet at 3.

28 ANPRM at 18-19.

29 ANPRM at 18. For an example of the demographic exception, see Example 3, ANPRM at 20-21.

30 Example 2, ANPRM at 20.

31 Example 7, ANPRM at 22.

32 ANPRM at 22.

33 ANPRM at 22 (emphasis added).

should be in the final rule, citing potential distances of 1,750 or 1,850 feet based on certain state data-privacy laws.[34]

(iii) Biometric identifiers: The ANPRM contemplates that this means "measurable physical characteristics or behaviors used to recognize or verify the identity of an individual" such as facial images, fingerprints or voice prints and patterns.[35]

(iv) Personal financial data: The ANPRM contemplates that this includes data about an individual's credit/debit or bank accounts, purchasing history, data in financial or bank statements, including assets, liabilities, debts and transactions, or data from a consumer's credit report. The ANPRM leaves open whether certain categories, such as "trade secrets" or "proprietary information" that do not relate to an individual, personal communications, or publicly available data should be excluded from this category.[36]

(v) Human genomic data.[37]

(vi) Personal health data.[38]

"Sensitive personal data" does *not* include (i) "data that is a matter of public record" (e.g. court records) as well as (ii) certain "personal communications" and "information or informational materials" that are expressly excluded from the scope of IEEPA under the 'Berman Amendment.'[39] DOJ contemplates that it will provide a regulatory definition on the scope of the "informational materials" provision by interpreting it to include "expressive information, like videos and artwork" and "*excluding* non-expressive data."[40]

---

34 Question 10, ANPRM 27-28.

35 ANPRM at 22.

36 ANPRM at 23.

37 ANPRM at 23. While the Order permits a broader regulation of "human 'omic data" after the submission of a report coordinated through the NSC on the "risks and benefits" of such regulation, DOJ, for now, contemplates only regulating human genomic data. Order § 6.

38 ANPRM at 23.

39 Order § 7(l); 50 U.S.C. § 1702(b)(1) (excluding "any postal, telegraphic, telephonic, or other personal communication, which does not involve a transfer of anything of value"); 50 U.S.C. 1702(b)(3) (excluding "whether commercial or otherwise, regardless of format or medium of transmission, of any information or informational materials, including but not limited to, publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds").

40 ANPRM at 23-24 (emphasis added). This provision will mark a significant regulatory development on the scope of IEEPA. Though these regulations will not directly apply to the sanctions programs administered by the Department of the Treasury's Office of Foreign Assets Control ("OFAC"), the regulatory definitions here could inform how OFAC considers these issues as it has not provided detailed regulations on these issues before. And this may ultimately become an area where plaintiffs seek to ultimately challenge the regulation by arguing that the restrictions on "non-expressive" transfers of data indirectly restrict expressive activity. In 2020, a federal court in the Eastern District of Pennsylvania granted a preliminary injunction blocking the enforcement of President Trump's Executive Order pursuant to IEEPA that effectively banned Tiktok. The court held that the Executive Order exceeded the scope of IEEPA because it was "an indirect regulation" of the expressive materials that were created on Tiktok. *Marland* v. *Trump*, 498 F. Supp. 3d 624, 641 (E.D. Pa. 2020).

(b) Bulk Thresholds

The ANPRM anticipates regulating transactions involving the aforementioned six categories of sensitive personal data only if they meet certain prescribed bulk volumes (i.e. a threshold number of U.S. persons or devices). The ANPRM contemplates potential thresholds as follows, measured by grouping transactions with the same party over the preceding twelve months:[41]

	Human Genomic Data	***Biometrics Identifiers***	***Precise Geolocation Data***	***Personal Health Data***	***Personal Financial Data***	***Covered Personal Identifiers***
Low	More than 100 *U.S. persons*	More than 100 *U.S. persons* (for *biometrics identifiers*) or U.S. devices (for *precise geolocation data*)		More than 1,000 *U.S. persons*		More than 10,000 *U.S. persons*
High	More than 100 *U.S. persons*	More than 100 *U.S. persons* (for *biometrics identifiers*) or U.S. devices (for *precise geolocation data*)		More than 1,000,000 *U.S. persons*		More than 1,000,000 *U.S. persons*

These bulk thresholds will *not* apply to "transactions involving certain U.S. Government-related data," described below, which are regulated "regardless of the volume of such data."[42]

(c) U.S. Government-related data

In addition to restricting transactions of sensitive personal data, the Order restricts transactions involving "United States Government-related data."[43] DOJ contemplates defining that as:

(i) *Location Data*: "any precise geolocation data, regardless of volume, for any location within any area enumerated on a list of specified geofenced areas associated with military, other government, or other sensitive facilities or locations." That list will be known as the "Government-Related Location Data List" and will be published by DOJ following an interagency process.[44]

(ii) *Sensitive Personal Data*: "any sensitive personal data, regardless of volume, that a transaction party markets as linked or linkable to current or recent former employees or contractors, or former senior officials of the U.S. government[.]"[45]

41 ANPRM at 25.

42 Fact Sheet at 3.

43 Order § 7(m).

44 ANPRM at 30.

45 ANPRM at 30.

3. Covered Data Transactions

The ANPRM contemplates two categories of covered data transactions—prohibited transactions and restricted transactions (which require certain mitigation measures). The ANPRM contemplates the prohibitions or restrictions applying prospectively to any relevant transaction that "was initiated, is pending, or will be completed after the effective date of the [DOJ] regulations."[46]

(a) Prohibited Transactions

The ANPRM contemplates prohibiting "data-brokerage transactions."[47] Data brokerage transactions include a sale, licensing of access, or other type of commercial transaction that involves 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."[48] That includes transactions where the provider sells or provides access (*e.g.*, through a subscriptive service or license) to bulk sensitive U.S. personal data or U.S. government-related data.[49]

(b) Restricted Transactions

The ANPRM contemplates identifying three categories of restricted data transactions: (1) vendor agreements involving the provision of goods and services (including cloud-service agreements); (2) employment agreements; and (3) investment agreements.[50]

1. *Vendor Agreements*: These are defined as arrangements or agreements involving the provision of goods or services by one person to another, including cloud-computing (IaaS, SaaS, PaaS) services, for payment or other consideration, exclusive of all Employment Agreements. An agreement between a U.S. company that collects bulk precise geolocation data and a service provider headquartered in a Country of Concern for processing and storage of that data, or simply with access to that data, would be a Vendor Agreement covered by the ANPRM.[51] Similarly, an agreement between a U.S. managed services provider owned by a foreign entity from a Country of Concern and its customers storing bulk U.S. sensitive personal data in the managed services provider's U.S. data center would be a Vendor Agreement.[52] The ANPRM specifies that certain services performed under a Vendor Agreement may not be covered data transactions subject to regulation if they do not "involve" the bulk U.S. sensitive personal data.[53]

2. *Employment Agreements*: The ANPRM defines these as any agreement or arrangement in which an individual performs work or job functions directly for a person in exchange for payment, professional opportunity or other consideration. Covered Employment Agreements would include agreements between individuals from a Country of Concern and a U.S.

46 ANPRM at 47.

47 Fact Sheet at 3. The ANPRM also contemplates prohibiting genomic-data transactions involving the transfer of bulk human genomic data or biospecimens from which such data can be derived.

48 ANPRM at 34.

49 ANPRM at 34.

50 Fact Sheet at 3.

51 Examples 19 and 20, ANPRM at 35

52 Example 21, ANPRM at 35.

53 Example 23, ANPRM at 35-36.

Company that has hired them to provide back-end services, which includes access to bulk human genomic data from U.S. consumers.[54]

3. *Investment Agreements*: The ANPRM defines these as any agreement or arrangement where a person obtains an ownership interest in real estate or a U.S. legal entity. Investment Agreements that would be covered under the ANPRM would include an agreement by a foreign private equity fund located in a Country of Concern to provide capital for the construction of a U.S. data center by a U.S. company that would store bulk personal health data on U.S. persons in exchange for a majority stake of ownership in the data center.[55] An agreement between a foreign technology company subject to jurisdiction of a Country of Concern to acquire a minority stake in a U.S. business which offers products that collect bulk U.S. sensitive personal data of U.S. users would be covered under the ANPRM regardless of whether the agreement gives the foreign company the ability to access this data. Even where access to bulk U.S. sensitive personal data is restricted in an Investment Agreement, it "would still fall into the class of restricted covered data transactions that have been determined to pose an unacceptable risk to national security because they may enable Countries of Concern or Covered Persons to access the bulk U.S. sensitive personal data." The degree of risk of access to this data under the specific Investment Agreement "does not affect whether the agreement is restricted."[56]

These restricted transactions will be subject to certain "security requirements" to be established by CISA. DOJ notes that the "security requirements will be designed to mitigate the risk of access by countries of concern or covered persons and may include cybersecurity measures such as basic organizational cybersecurity posture requirements, physical and logical access controls, data masking and minimization, and the use of privacy-preserving technologies."[57]

(c) Re-Export Certification Requirement

The ANPRM has a specific provision to "address the risk that data is 're-exported' by foreign third parties to countries of concern."[58]

ANPRM contemplates that a U.S. person would be prohibited from engaging in "a covered data transaction involving data brokerage with any foreign person unless the U.S. person contractually requires that the foreign person refrain from engaging in a subsequent covered data transaction involving the same data with a country of concern or a covered person."[59]

That would prohibit U.S. companies from engaging in data brokerage agreements with *any* foreign company unless the foreign company signs this certification.

(d) Exemptions

The ANPRM contemplates that there would be certain categories of data transactions that would be entirely excluded from the scope of the regulation.[60] In relevant part, these include covered data transactions that are:

54 Example 24, ANPRM at 36.

55 Example 28, ANPRM at 37.

56 Examples 29-30, ANPRM at 37.

57 Fact Sheet at 4.

58 Fact Sheet at 6.

59 ANPRM at 50.

60 Fact Sheet at 4.

(i) ordinarily incident to and part of financial services, payment processing, and regulatory compliance;

(ii) ordinarily incident to and part of ancillary business operations (such as payroll or human resources) *within* multinational U.S. companies.

The ANPRM also contemplates "exempting certain investments that do not convey the rights or influence that ordinarily pose an unacceptable national-security risk of giving countries of concern or covered persons access to sensitive personal data."[61]

4. Licensing and Advisory Opinions

The ANPRM contemplates that DOJ will issue certain licenses and advisory opinions. This will be similar to the processes utilized by OFAC in administering U.S. sanctions programs. This will include general licenses that broadly permit otherwise prohibited or restricted transactions as well as specific licenses that a company can apply for to obtain authorization for a specific transaction. DOJ also contemplates that companies will be able to apply for "advisory opinions" where DOJ will provide an opinion on the application of the regulations for a specific transaction.[62]

5. Penalties and Reporting/Recordkeeping Requirements

The ANPRM proposes the establishment of civil penalties for violations. DOJ proposes that the violation would have to satisfy a "knowingly" requirement, which DOJ defines as including where the person "should have known" of the violation.[63] The ANPRM also states that it is considering regulations, similar to other IEEPA-based regulations, that will prohibit "evasions, causing violations, attempts, and conspiracies."[64] The reference to "causing violations" suggests that DOJ contemplates being able to take enforcement actions (as OFAC has done in the sanctions context) against foreign persons for "causing" violations by U.S. persons.

DOJ notes that U.S. persons will be expected to develop compliance programs based on their risk factors and that DOJ "would consider the adequacy of the compliance program in any enforcement action."[65]

The ANPRM also contemplates that certain persons would be subject to affirmative reporting obligations. Persons granted a license would be required to provide annual certifications "that they have abided by the terms of any license granted." Additionally, the ANPRM contemplates affirmative reporting obligations for a U.S. person that is "(a) engaged in restricted covered data transactions involving cloud computing services or licensed covered data transactions involving data brokerage or cloud-computing services, and (b) has 25 percent or more of its equity interests owned (directly or indirectly, through any contract, arrangement, understanding, relationship, or otherwise) by a country of concern or covered person;" or any U.S. person that "has received and affirmatively rejected an offer from another person to engage in a prohibited covered data transaction involving data brokerage."[66]

Implications

The Executive Order marks another instance where the President is turning to authority under IEEPA to, in effect, create a significant new regulatory regime. Here, DOJ has been charged with undertaking a significant new role in setting up and

61 Fact Sheet at 4.

62 Fact Sheet at 4.

63 ANPRM at 48.

64 ANPRM at 51.

65 Fact Sheet at 7.

66 ANPRM at 69-70.

administering this regulatory regime. While the focus right now will be on the regulatory process, DOJ will ultimately need to establish the infrastructure to review licenses and undertake civil enforcement cases—measures that, in large respect, are more akin to what OFAC has done in administering the sanctions regime.

The Order and ANPRM mark the beginning of a significant rule-making process. The Order instructs DOJ to publish a proposed rule (an NPRM) within 180 days with a final rule be issued thereafter. With the ANPRM, DOJ has solicited public comments on many critical definitions that it is contemplating including in the proposed rule, which provides regulated industries an opportunity to engage with the government and shape the proposed rule and the ultimate final rule.

While the Order and ANPRM do not impose any new regulatory requirements immediately, they clearly signal that the United States intends to impose significant restrictions on transactions involving a broad array of "sensitive" U.S. personal data. Moreover, the Order makes clear that this is a *national security* regulation—done under the same legal basis as U.S. sanctions—and once regulations are issued DOJ will likely be seeking to bring enforcement actions against companies that violate these regulations.

Given the expansive definition of sensitive personal data, the rule's prohibitions may broadly curtail the types of partnerships and arrangements that U.S. companies are able to engage in with Chinese companies. Additionally, the restrictions on employment, vendor and investment agreements will require careful attention to compliance for companies that have such agreements with covered persons. In complying with those obligations, U.S. companies will need to ensure that they are diligently following the "security requirements" that CISA will issue.

DOJ has made clear that companies will be "expected to develop and implement compliance programs" that reflect their "individualized risk profiles" taking into account their "products and services, customers and counterparties, and geographic locations."[67] As an initial step, U.S. companies that hold bulk sensitive U.S. personal data—and covered persons that have ongoing or contemplated arrangements that access such data--should consider understanding the implications for business lines and compliance programs.

* * *

[67] Fact Sheet at 7.

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

L. Rush Atkinson
+1-202-223-7473
ratkinson@paulweiss.com

John P. Carlin
+1-202-223-7372
jcarlin@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

Peter Carey
+1-202-223-7485
pcarey@paulweiss.com

David K. Kessler
+1-212-373-3614
dkessler@paulweiss.com

Nathan Mitchell
+1-202-223-7422
nmitchell@paulweiss.com

Associates Sarah Calderone, Matthew J. Disler, Samuel Kleiner, Sean S. Malone, Cole A. Rabinowitz, Joshua R. Thompson, Jacob Wellner and Simona Xu contributed to this Client Memorandum.