Note: This is the text of the Data Security Advance Notice of Proposed Rulemaking (ANPRM) as signed by the Assistant Attorney General for National Security. The official version of the ANPRM will be published in the Federal Register.

DEPARTMENT OF JUSTICE

National Security Division

28 CFR Part 202

[Docket No. NSD 104]

RIN 1105-AB72

Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern

AGENCY: National Security Division, Department of Justice.

ACTION: Advance notice of proposed rulemaking.

SUMMARY: The Executive Order of February 28, 2024, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" (the Order), directs the Attorney General to issue regulations that prohibit or otherwise restrict United States persons from engaging in any acquisition, holding, use, transfer, transportation, or exportation of, or dealing in, any property in which a foreign country or national thereof has any interest ("transaction"), where the transaction: (a) involves U.S. government-related data or bulk U.S. sensitive personal data, as defined by final rules implementing the Order; (b) falls within a class of transactions that has been determined by the Attorney General to pose an unacceptable risk to the national security of the United States because it may enable access by countries of concern or covered persons to Americans' bulk sensitive personal data or U.S. government-related data; and (c) meets other criteria specified by the Order. This advance notice of proposed rulemaking (ANPRM) seeks public comment on various topics related to the implementation of the Order.

Note: This is the text of the Data Security Advance Notice of Proposed Rulemaking (ANPRM) as signed by the Assistant Attorney General for National Security. The official version of the ANPRM will be published in the Federal Register.

DATES: Written comments on this ANPRM must be received by **[INSERT DATE 45 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**.

ADDRESSES: You may send comments, identified by Docket No. NSD 104, by either of the following methods:

• *Federal eRulemaking Portal*: https://www.regulations.gov. Follow the instructions for sending comments.

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

Instructions: We encourage comments to be submitted via *https://www.regulations.gov.* Please submit comments only and include your name and company name (if any) and cite "Provisions Pertaining to Preventing Access to Americans' Bulk Sensitive Personal Data and U.S. Government-Related Data by Countries of Concern" in all correspondence. Anyone submitting business confidential information should clearly identify the business confidential portion at the time of submission, file a statement justifying nondisclosure and referring to the specific legal authority claimed, and provide a non-confidential version of the submission. For comments submitted electronically containing business confidential information, the file name of the business confidential version should begin with the characters "BC." Any page containing business confidential information must be clearly marked "BUSINESS CONFIDENTIAL" at the top of that page. The corresponding non-confidential version of those comments must be clearly marked "PUBLIC." The file name of the nonconfidential version should begin with the character "P." Any submissions with file names that do not begin with either a "BC" or a "P" will be assumed to be public and

will be posted without change, including any business or personal information provided, such as names, addresses, email addresses, or telephone numbers.

To facilitate an efficient review of submissions, the Department of Justice encourages but does not require commenters to: (1) submit a short executive summary at the beginning of all comments; (2) provide supporting material, including empirical data, findings, and analysis in reports or studies by established organizations or research institutions; (3) consistent with the questions below, describe the relative benefits and costs of the approach contemplated in this ANPRM and any alternative approaches; and (4) refer to the numbered question(s) herein to which each comment is addressed. The Department of Justice welcomes interested parties' submissions of written comments discussing relevant experiences, information, and views. Parties wishing to supplement their written comments in a meeting may request to do so, and the Department of Justice may accommodate such requests as resources permit. Additionally, in consultation with other United States Government agencies, the Department of Justice expects to seek additional opportunities to engage in discussions with certain stakeholders, including foreign partners and allies.

FOR FURTHER INFORMATION CONTACT: Email (preferred): NSD.FIRS.datasecurity@usdoj.gov. Otherwise, please contact: Lee Licata, Deputy Chief for National Security Data Risks, Foreign Investment Review Section, National Security Division, U.S. Department of Justice, 175 N Street NE, Washington, DC 20002; telephone: 202-514-8648.

SUPPLEMENTARY INFORMATION:

I. Background

On February 28, 2024, the President issued the Order pursuant to his authority under the Constitution and laws of the United States, including the International Emergency Economic Powers Act (50 U.S.C. §§ 1701 et seq.) (IEEPA), the National Emergencies Act (50 U.S.C. §§ 1601 et seq.) (NEA), and section 301 of Title 3, United States Code. In the Order, the President expanded the scope of the national emergency declared in Executive Order 13873 of May 15, 2019 (Securing the Information and Communications Technology and Services Supply Chain), and further addressed with additional measures in Executive Order 14034 of June 9, 2021 (Protecting Americans' Sensitive Data from Foreign Adversaries). The President determined that additional measures are necessary to counter the unusual and extraordinary threat to U.S. national security posed by the continuing efforts of certain countries of concern to access and exploit Americans' bulk sensitive personal data and U.S. Government-related data ("government-related data").

Unrestricted transfers of bulk sensitive personal data and government-related data to countries of concern, through commercial transactions or otherwise, present a range of threats to U.S. national security and foreign policy. Countries of concern can use their access to Americans' bulk sensitive personal data to engage in malicious cyber-enabled activities and malign foreign influence, and to track and build profiles on U.S. individuals, including members of the military and Federal employees and contractors, for illicit purposes such as blackmail and espionage. Countries of concern can also use access to U.S. persons' bulk sensitive personal data to collect information on activists,

academics, journalists, dissidents, political figures, or members of non-governmental organizations or marginalized communities in order to intimidate such persons; curb political opposition; limit freedoms of expression, peaceful assembly, or association; or enable other forms of suppression of civil liberties.

The Office of the Director of National Intelligence (ODNI) has made clear that "[o]ur adversaries increasingly view data as a strategic resource. They are focused on acquiring and analyzing data—from personally identifiable information on U.S. citizens to commercial and government data—that can make their espionage, influence, kinetic and cyber-attack operations more effective; advance their exploitation of the U.S. economy; and give them strategic advantage over the United States."[1] Advanced technologies—including big-data analytics, artificial intelligence (AI), high-performance computing, and other capabilities—increasingly enable countries of concern to exploit bulk amounts of Americans' sensitive personal data and government-related data to achieve these goals.

As ODNI has assessed, countries of concern are "increasing their ability to analyze and manipulate large quantities of personal information in ways that will allow them to more effectively target and influence, or coerce, individuals and groups in the United States and allied countries."[2] Countries of concern "almost certainly are already applying data-analysis techniques to hone their efforts against U.S. targets."[3] For

---

[1] Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* at 26 (Feb. 6, 2023), https://www.odni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf [https://perma.cc/4B2Y-7NVD].

[2] National Intelligence Council, *Assessment: Cyber Operations Enabling Expansive Digital Authoritarianism* at 3 (Apr. 7, 2020) (declassified Oct. 5, 2022), https://www.dni.gov/files/ODNI/documents/assessments/NICM-Declassified-Cyber-Operations-Enabling-Expansive-Digital-Authoritarianism-20200407--2022.pdf [https://perma.cc/ZKJ4-TBU6].

[3] *Id.*

example, AI is making it easier to extract, re-identify, link, infer, and act on sensitive information about people's identities, locations, habits, and desires, as outlined in Executive Order 14110 of October 30, 2023 (Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence).[4] Likewise, as the National Counterintelligence and Security Center has explained, "[t]he combination of stolen [personally identifiable information], personal health information, and large [human] genomic data sets collected from abroad" gives countries of concern "vast opportunities to precisely target individuals in foreign governments, private industries, or other sectors for potential surveillance, manipulation, or extortion."[5] Moreover, access to bulk sensitive personal data can fuel the creation and refinement of AI, big-data, and other analytical capabilities, the development of which requires large amounts of human data—ultimately compounding the risks.

These risks are not merely hypothetical and have been tested. As a recent study has explained, for example, "[a]ggregated insights from location data" could be used to damage national security[6]—such as in 2018, when the publication of a global heatmap of users' location data collected by a popular fitness app enabled researchers to quickly

[4] *See also id.* at 4–5 (explaining that China's "commercial access to personal data of other countries' citizens, along with AI-driven analytics," can "enable it to automate the identification of individuals and groups," and "China can draw on ample Western commercial models for large-scale algorithm-driven delivery of targeted content and behavior-shaping microincentives").

[5] National Counterintelligence and Security Center, *China's Collection of Genomic and Other Healthcare Data From America: Risks to Privacy and U.S. Economic and National Security* at 4 (Feb. 2021), https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/NCSC_China_Genomics_Fact_Sheet_2021revision20210203.pdf [https://perma.cc/BL4H-WJSW].

[6] Justin Sherman et al., *Data Brokers and the Sale of Data on U.S. Military Personnel* at 15 (Nov. 2023), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/11/Sherman-et-al-2023-Data-Brokers-and-the-Sale-of-Data-on-US-Military-Personnel.pdf [https://perma.cc/M9S8-MYAA].

identify and map the locations of military and government facilities and activities.[7] Similarly, in 2019, New York Times writers were able to combine a single set of bulk location data collected from cell phones and bought and sold by location-data companies—which was anonymized and represented "just one slice of data, sourced from one company, focused on one city, covering less than one year"—with publicly available information to identify, track, and follow "military officials with security clearances as they drove home at night," "law enforcement officers as they took their kids to school," and "lawyers (and their guests) as they traveled from private jets to vacation properties."[8]

Countries of concern can also exploit access to government-related data, regardless of volume. As one report has explained, for example, tracking location data on individual military or government targets can "reveal sensitive locations—such as visits to a place of worship, a gambling venue, a health clinic, or a gay bar—which again could be used for profiling, coercion, blackmail, or other purposes," or could reveal "reputationally damaging lifestyle characteristics" that could be exploited, "such as infidelity."[9]

Accordingly, transactions that may enable countries of concern to access bulk amounts of Americans' sensitive personal data or government-related data, as defined by the Order, pose particular and unacceptable risks to national security and foreign policy. This risk of access to U.S. persons' bulk sensitive personal data and government-related

---

[7] *E.g.*, Richard Pérez-Peña and Matthew Rosenberg, *Strava Fitness App Can Reveal Military Sites, Analysts Say*, The New York Times (Jan. 29, 2018), https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html [https://perma.cc/VZF9-X7LJ]; Jeremy Hsu, *The Strava Heat Map and the End of Secrets*, WIRED (Jan. 29, 2018 7:14 PM), https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy [https://perma.cc/B9KT-E75J].

[8] Stuart A. Thompson and Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, The New York Times (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html [https://perma.cc/X3VB-429P].

[9] Sherman et al., *supra* note 6, at 15.

data is not limited to transactions directly involving the governments of countries of concern. Persons who are owned by, controlled by, or subject to the jurisdiction or direction of a country of concern may enable the government of that country to indirectly access such data. For example, countries of concern may have cyber, national security, and intelligence laws that, without sufficient legal safeguards, can obligate such persons to provide that country's intelligence services access to U.S. persons' bulk sensitive personal data and government-related data.

Countries of concern can leverage their access to Americans' bulk sensitive personal data and government-related data to engage in a variety of nefarious activities, including malicious cyber-enabled activities, espionage, and blackmail. Countries of concern can exploit Americans' bulk sensitive personal data and government-related data to track and build profiles on U.S. persons, including Federal employees and contractors, military servicemembers, and members of the Intelligence Community to support espionage operations and to identify and exploit vulnerabilities for malicious cyber activities. Countries of concern can also access U.S. persons' bulk sensitive personal data and government-related data to collect information on activists, academics, journalists, dissidents, political figures, and members of non-governmental organizations and marginalized communities to intimidate opponents of countries of concern, curb dissent, and limit Americans' freedom of expression and other civil liberties. The risks posed by access to Americans' bulk sensitive personal data and government-related data are exacerbated by AI and other data processing tools that exploit large datasets in increasingly sophisticated and effective ways to the detriment of U.S. national security. These tools, and the access to Americans' bulk sensitive personal data and government-

related data upon which the tools rely, enable countries of concern to target U.S. persons more effectively by recognizing patterns across multiple, unrelated datasets to identify individuals whose links to, for example, the Federal Government, would be otherwise obscured in a single database.

As the President affirmed in the Order, the United States remains committed to promoting an open, global, interoperable, reliable, and secure Internet; promoting open, responsible scientific collaboration to drive innovation; protecting human rights online and offline; supporting a vibrant, global economy by promoting cross-border data flows to enable international commerce and trade; and facilitating open investment. Accordingly, the Order authorizes the Attorney General to take specific, carefully calibrated actions to minimize the risks associated with access to Americans' bulk sensitive personal data and government-related data by countries of concern and persons that are "owned by, controlled by, or subject to the jurisdiction or direction of" countries of concern, while minimizing disruption to commercial activity. For example, the Order exempts certain classes of transactions that are less likely to pose these unacceptable national-security risks, including financial-services transactions, and authorizes the Attorney General to exempt additional classes of transactions. Also consistent with the Order, this ANPRM does not propose generalized data-localization requirements either to store Americans' bulk sensitive personal data or government-related data within the United States or to locate computing facilities used to process Americans' bulk sensitive personal data or government-related data within the United States. Nor does it seek to broadly prohibit U.S. persons from conducting commercial transactions with entities and individuals located in countries of concern or impose measures aimed at a broader

decoupling of the substantial consumer, economic, scientific, and trade relationships that the United States has with other countries. This carefully calibrated action instead reflects the U.S. Government's longstanding support for the concept of "Data Free Flow with Trust," in recognition of its importance to the economy and human rights online.

The Order has two primary components relevant to this ANPRM. First, it directs the Attorney General, in coordination with the Secretary of Homeland Security and in consultation with the relevant agencies, to issue regulations identifying for prohibition specific classes of transactions that may enable access by countries of concern or covered persons to defined categories of Americans' bulk sensitive personal data or government-related data, and that the Attorney General determines pose an unacceptable risk to U.S. national security and foreign policy. Second, it instructs the Attorney General, in coordination with the Secretary of Homeland Security and in consultation with the relevant agencies, to issue regulations identifying specific classes of transactions that will be required to comply with security requirements, to be established by the Secretary of Homeland Security through the Director of the Cybersecurity and Infrastructure Security Agency, that mitigate the risks of access to Americans' bulk sensitive personal data or government-related data by countries of concern. As previewed in this ANPRM, the security requirements could include (1) organizational requirements (e.g., basic organizational cybersecurity posture), (2) transaction requirements (e.g., data minimization and masking, use of privacy-preserving technologies, requirements for

information-technology systems to prevent unauthorized disclosure, and logical and physical access controls), and (3) compliance requirements (e.g., audits).[10]

II. Program Overview

The Department of Justice is considering implementing the Order through categorical rules that regulate certain data transactions involving bulk U.S. sensitive personal data and government-related data that present an unacceptable risk to U.S. national security, pursuant to section 2(c) of the Order. To that end, the Department of Justice is considering establishing a program that would (1) identify certain classes of highly sensitive transactions that would be prohibited in their entirety ("prohibited transactions"), and (2) identify other classes of transactions that would be prohibited except to the extent they comply with predefined security requirements ("restricted transactions") to mitigate the risk of access to bulk sensitive personal data by countries of concern.

Under this framework, the Department of Justice would establish the program by issuing proposed rulemakings in tranches based on priority, including the limits of current authorities, and effective administration of the program. This ANPRM takes the foundational steps by seeking the input needed to establish the structure of the program, including, as described in section 2(c) of the Order, identifying classes of prohibited and restricted transactions that pose an unacceptable risk to national security, defining relevant terms, identifying countries of concern, creating processes for administrative

[10] The Order contains other provisions, which are not directly relevant to this ANPRM, to enhance existing authorities to address data-security risks, including directing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector to take certain actions with respect to submarine cables; instructing the Secretaries of Defense, Health and Human Services, and Veterans Affairs, and the Director of the National Science Foundation, to consider taking certain steps regarding the provision of Federal assistance; and encouraging the Consumer Financial Protection Bureau to take consider taking steps to address the role that data brokers play in contributing to the national-security risks.

licensing and entity designations, and establishing a compliance and enforcement regime. This ANPRM is focused on identifying discrete classes of prohibited transactions that raise the highest national-security risks, focusing on data transactions between U.S. persons and countries of concern (or persons subject to their ownership, control, jurisdiction, or direction where the transaction involves property in which a foreign country or national thereof has an interest) that pose direct risks. As contemplated by this ANPRM, the rulemaking would target only transactions between a U.S. person and a country of concern (or person subject to its ownership, control, jurisdiction, or direction), with one discrete exception described below. The program would not regulate purely domestic transactions between U.S. persons (who are not otherwise designated as covered persons acting on behalf of a country of concern), such as the collection, maintenance, processing, or use of data by U.S. persons within the United States.

Section 2(f) of the Order authorizes the Department of Justice to engage in subsequent rulemakings to tailor the regulatory program to the national-security risks identified in the Order, and to the costs and benefits of administering and complying with the regulatory program. Where practical, the proposed program, its structure, and definitions would be modeled on existing regulations based on IEEPA that are generally familiar to the public, such as those administered by the United States Department of the Treasury's Office of Foreign Assets Control (OFAC) and the United States Department of Commerce's Bureau of Industry and Security (BIS).

Under section 2(a)(ii) of the Order, the Attorney General is authorized to determine and identify classes of transactions that "pose an unacceptable risk to the national security of the United States because the transactions may enable countries of

concern or covered persons to access bulk sensitive personal data or United States Government-related data." Specifically, the Department of Justice is considering identifying two classes of prohibited data transactions between U.S. persons and countries of concern (or covered persons) to address critical risk areas involving bulk U.S. sensitive personal data or government-related data: (1) data-brokerage transactions; and (2) any transaction that provides a country of concern or covered person with access to bulk human genomic data (a subcategory of human 'omic data) or human biospecimens from which that human genomic data can be derived. These classes of prohibited data transactions are not directly regulated under existing Federal authorities, and these types of transactions necessarily provide access to bulk sensitive personal data or government-related data directly to countries of concern or persons subject to their ownership, control, jurisdiction, or direction.

The Department of Justice is also considering identifying three classes of restricted data transactions to address critical risk areas to the extent they involve countries of concern or covered persons and bulk U.S. sensitive personal data: (1) vendor agreements (including, among other types, agreements for technology services and cloud-service agreements), (2) employment agreements, and (3) investment agreements. These classes of restricted transactions represent significant means through which countries of concern can access bulk U.S. sensitive personal data or government-related data, but the national-security risks associated with these transactions can be mitigated through appropriate security-related conditions.

The program would cover transactions involving six defined categories of bulk U.S. sensitive personal data—U.S. persons' covered personal identifiers, personal

financial data, personal health data, precise geolocation data, biometric identifiers, and human genomic data—and combinations of those categories, as laid out in the Order and defined below. These categories would be clearly defined and, for covered personal identifiers, significantly narrower than the broad categories of material typically implicated by privacy-focused regulatory regimes.

In addition to addressing data transactions involving bulk U.S. sensitive personal data, and as also laid out in the Order, the program would also address the heightened national-security risks posed by U.S. persons' transactions with countries of concern (or covered persons) and two kinds of government-related data regardless of volume: (1) geolocation data in listed geofenced areas associated with certain military, other government, and other sensitive facilities (which could threaten national security by revealing information about those locations and U.S. persons associated with them), and (2) sensitive personal data that is marketed as linked or linkable to current or recent former employees or contractors, or former senior officials, of the U.S. government, including the military and Intelligence Community.

Consistent with the Order, the program would be implemented as a carefully calibrated national-security authority to address specific national security threats, including counterintelligence threats, posed by data-security risks to U.S. persons and government-related data. The program is not intended as a commercial regulation of all cross-border data flows between the United States and our foreign partners, or as a comprehensive program to regulate Americans' data privacy. Also consistent with the Order, the Department of Justice intends to implement the program consistent with longstanding U.S. policy to promote trusted cross-border data transfers among partners

that respect democratic values and the rule of law, as the program would address only the national-security risks posed by countries of concern because of their potential to target and misuse Americans' sensitive personal data.

Importantly, the program is also not intended to impede all U.S. persons' data transactions with countries of concern or persons subject to their jurisdiction. The program, under the rulemaking under consideration, would prohibit or restrict specific classes of data transactions between U.S. persons and countries of concern (or persons subject to their ownership, control, jurisdiction, or direction) that involve either (1) specific categories of sensitive personal data above certain bulk-volume thresholds or (2) specific categories of government-related data regardless of volume. The program under consideration would also identify classes of exempt data transactions and would provide a process for the Department of Justice to issue general and specific licenses using procedures that are generally familiar to the public.

The Department of Justice does not contemplate that the program will rely on case-by-case review of individual data transactions. Rather, the Department of Justice will affirmatively identify classes of prohibited and restricted data transactions. Importantly, the Department of Justice believes that a categorical approach provides bright-line rules to data-transaction parties. The program would not apply retroactively (before the effective date of the final rule). However, the Department of Justice may, after the effective date of the regulations, request information about transactions by United States persons that were completed or agreed to after the date of the issuance of the Order to better inform the development and implementation of the program.

III. Issues for Comment

The Department of Justice welcomes comments and views from a wide range of stakeholders on all aspects of how the Attorney General should implement this new program under the Order. The Department of Justice is particularly interested in obtaining information on the topics discussed below. This ANPRM does not necessarily identify the full scope of potential approaches the Department of Justice might ultimately undertake in regulations to implement the Order.

A. Overview

The Order frames the key terms that will be developed through rulemaking. Under the rules that the Department of Justice is considering, *U.S. persons* would be prohibited from engaging in classes of *covered data transactions*, which (as further defined below) have been determined by the Attorney General to pose an unacceptable risk to the national security of the United States because these classes of *covered data transactions* may enable *countries of concern* or *covered persons* to *access bulk U.S. sensitive personal data* or *government-related data*. Some otherwise-prohibited *covered data transactions* may be restricted and be permitted to proceed only subject to certain conditions, including *security requirements* published by the Department of Homeland Security in coordination with the Department of Justice. Prohibited or restricted *covered data transactions* may also be permitted to proceed based on applicable general or specific licenses. None of the program's requirements would apply to a *U.S. person* engaged in an exempt data *transaction*.

Definitions under consideration for these and related terms are italicized and discussed below, along with questions on which the Department of Justice seeks comment.

B. Bulk U.S Sensitive Personal Data

The Order authorizes the Attorney General to prohibit or otherwise restrict United States persons from engaging in any transaction where the transaction involves bulk sensitive personal data and meets other criteria specified in section 2(a) of the Order. The Order defines "bulk" as "an amount of sensitive personal data that meets or exceeds a threshold over a set period of time, as specified in regulations issued by the Attorney General pursuant to section 2 of th[e] order." The Order also 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," as further defined in final rules implementing the Order, "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." The Department of Justice is considering elaborating on and providing greater detail to the Order's definitions of "sensitive personal data" and "bulk."

Sensitive personal data. The Department of Justice is considering further defining each of the six categories of *sensitive personal data* identified in the Order as follows:

1. *Covered personal identifiers*. The Order defines "covered personal identifiers" as "specifically listed classes of personally identifiable data that are reasonably linked to an individual, and that -- whether in combination with each other, with other sensitive

personal data, or with other data that is disclosed by a transacting party pursuant to the transaction and that makes the personally identifiable data exploitable by a country of concern -- could be used to identify an individual from a data set or link data across multiple data sets to an individual." The Department is considering further defining the term *covered personal identifiers* as follows.

1(a). With respect to the subcategory of listed classes of personally identifiable data "in combination with each other," the term *covered personal identifiers* would mean any *listed identifier* that is *linked* to any other *listed identifier*, except:

(a) the term *covered personal identifiers* does not include demographic or contact data that is *linked* only to other demographic or contact data; and

(b) the term *covered personal identifiers* does not include a network-based identifier, account-authentication data, or call-detail data that is *linked* only to other network-based identifier, account-authentication data, or call-detail data as necessary for the provision of telecommunications, networking, or similar services.

Listed identifiers would include the following classes of data determined by the regulations to be "reasonably linked to an individual" under the Order's definition of "covered personal identifiers." The final rule will include a comprehensive list of *listed identifiers.*

- Full or truncated government identification or account number (such as a Social Security Number, driver's license or state identification number, passport number, or Alien Registration Number)
- Full financial account numbers or personal identification numbers associated with a financial institution or financial-services company
- Device-based or hardware-based identifier (such as International Mobile Equipment Identity (IMEI), Media Access Control (MAC) address, or Subscriber Identity Module (SIM) card number)
- Demographic or contact data (such as first and last name, birth date, birthplace, zip code, residential street or postal address, phone number, and email address and similar public account identifiers)
- Advertising identifier (such as Google Advertising ID, Apple ID for Advertisers, or other Mobile Advertising ID (MAID))

- Account-authentication data (such as account username, account password, or an answer to security questions)
- Network-based identifier (such as Internet Protocol (IP) address or cookie data)
- Call-detail data (such as Customer Proprietary Network Information (CPNI))

Under this definition, the term *covered personal identifiers* would be much narrower than the categories of material typically covered by laws and policies aimed generally at protecting personal privacy.[11] It would not include any combinations of types of data that are not expressly listed. For example, this definition of *covered personal identifiers* would not include an individual's:

- Employment history;
- Educational history;
- Organizational memberships;
- Criminal history; or
- Web-browsing history.

For purposes of defining *covered personal identifiers* only, the Department of Justice is considering defining identifiers as *linked* when the identifiers involved in a single *covered data transaction*, or in multiple *covered data transactions* or a course of dealing between the same or related parties, are capable of being associated with the same specific person(s). Identifiers would not be considered *linked* when additional identifiers or data not involved in the relevant *covered data transaction(s)* would be necessary to associate the identifiers with the same specific person(s). For example, if a *U.S. person* transferred two *listed identifiers* in a single spreadsheet—such as a list of

[11] *Cf., e.g.*, California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.140(v)(1) (defining "personal information" in the context of a generalized privacy-focused regime); Regulation (EU) 2016/679 of the European Parliament and of the Council, "On the protection of national persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC" (General Data Protection Regulation), art. 4(1) (27 April 2016) (defining "personal data" in the context of a generalized data privacy regime).

names of individuals and associated MAC addresses for those individuals' devices—the names and MAC addresses would be considered *linked*. The same would be true if the names and MAC addresses were transferred to two related parties in two different *covered data transactions*, provided that the receiving parties were capable of determining which names corresponded to which MAC addresses. On the other hand, a standalone list of MAC addresses, without any additional *listed identifiers*, would not be *covered personal identifiers*. That standalone list of MAC addresses would not become *covered personal identifiers* even if the receiving party is capable of obtaining separate sets of other *listed identifiers* or *sensitive personal data* through separate *covered data transactions* with unaffiliated parties that would ultimately permit the association of the MAC addresses to specific persons. The MAC addresses would not be considered *linked* to those separate sets of other *listed identifiers* or *sensitive personal data*.

The Department of Justice currently intends the category of *covered personal identifiers* to apply as follows:

- *Example 1.* A standalone *listed identifier* in isolation (i.e., that is not *linked* to another *listed identifier*, *sensitive personal data*, or 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) —such as a data set of only Social Security Numbers or only account usernames—would not constitute *covered personal identifiers*.

- *Example 2.* A *listed identifier linked* to another *listed identifier*—such as a data set of first and last names linked to Social Security Numbers, driver's license numbers linked to passport numbers, device MAC addresses linked to residential addresses, account usernames linked to first and last names, or mobile advertising IDs linked to email addresses—would constitute *covered personal identifiers*.

- *Example 3.* Demographic or contact data *linked* only to other demographic or contact data—such as a data set linking first and last names to residential street addresses, email addresses to first and last names, or customer loyalty membership records linking first and last names to phone

numbers—would not constitute *covered personal identifiers*.

- *Example 4.* Demographic or contact data *linked* to other demographic or contact data and to another *listed identifier*—such as a data set linking first and last names to email addresses and to IP addresses—would constitute *covered personal identifiers*.

- *Example 5.* Account usernames *linked* to passwords as part of a sale of a data set would constitute *covered personal identifiers*. Those types of account-authentication data are not linked as part of the provision of telecommunications, networking, or similar services.

1(b). With respect to the subcategory of listed classes of personally identifiable data "in combination ... with other sensitive personal data," the Department is considering treating these combinations as *combined data* subject to the lowest bulk threshold applicable to the categories of data present, as separately discussed below with respect to the definition of the term *bulk U.S. sensitive personal data*.

1(c). With respect to 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," the Department does not intend to impose an obligation on transacting parties to independently determine whether particular combinations of data would be "exploitable by a country of concern"; rather, the Department intends to identify specific classes of data that, when combined, would satisfy this standard. The Department seeks comment on other ways in which it can further define this subcategory. As context, the Department intends this subcategory to apply to scenarios such as the following:

- *Example 6.* A foreign person who is a *covered person* asks a U.S. company for a list of MAC addresses from devices that have connected to the wireless network of a U.S. fast-food restaurant located in a particular government building. The U.S. company then sells the list of MAC addresses, without any other *listed identifiers* or *sensitive personal data*, to the *covered person*. The data disclosed by the *covered person*'s inquiry for MAC addresses from "devices that have connected to the wireless network

of a U.S. fast-food restaurant located in a particular government building" makes the list of MAC addresses exploitable by a *country of concern*.

- *Example 7.* A U.S. company sells to a *country of concern* a list of full names that the company describes (in a heading in the list or to the *country of concern* as part of the transaction) as "members of a *country of concern's* opposition political party in New York City," or as "active-duty LGBTQ+ military officers" without any other *listed identifiers* or *sensitive personal data*. The data disclosed by the U.S. company's description of the list of names as "members of a *country of concern*'s opposition political party in New York City" or "active-duty LGBTQ+ military officers" makes the list of names exploitable by a *country of concern*.

By contrast, the Department does not intend this subcategory to apply to scenarios such as the following:

- *Example 8.* A *covered person* asks a U.S. company for a bulk list of birth dates for "any American who visited a Starbucks in Washington, D.C. in December 2023." The U.S. company then sells the list of birth dates, without any other *listed identifiers* or *sensitive personal data*, to the *covered person*.

- *Example 9.* A U.S. company sells to a *covered person* a list of full names that the company describes (in a heading in the list or to the *covered person* as part of the transaction) as "Americans who watched more than 50% of episodes" of a popular TV show, without any other *listed identifiers* or *sensitive personal data*.

2. *Geolocation and related sensor data.* The Department of Justice currently intends for its first rulemaking to regulate *covered data transactions* involving geolocation and related sensor data only to the extent that such *transactions* involve *precise geolocation data*. *Precise geolocation data* would mean 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.

3. *Biometric identifiers.* The term *biometric identifiers* means measurable physical characteristics or behaviors used to recognize or verify the identity of an individual,

including facial images, voice prints and patterns, retina and iris scans, palm prints and fingerprints, gait, and keyboard usage patterns that are enrolled in a biometric system and the templates created by the system.

4. *Human 'omic data.* The Department of Justice currently intends for its first rulemaking to regulate *covered data transactions* involving human 'omic data only to the extent that such *transactions* involve *human genomic data*. The term *human genomic data* means data representing the nucleic acid sequences that comprise the entire set or a subset of the genetic instructions found in a human cell, including the result or results of an individual's "genetic test" (as defined in 42 U.S.C. § 300gg-91(d)(17)) and any related human genetic sequencing data.

5. *Personal health data.* The term *personal health data* means "individually identifiable health information" (as defined in 42 U.S.C. § 1302d(6) and 45 CFR 160.103), regardless of whether such information is collected by a "covered entity" or "business associate" (as defined in 45 CFR 160.103).

6. *Personal financial data.* The term *personal financial data* means data about an individual's credit, charge, or debit card, or bank account, including purchases and payment history; data in a bank, credit, or other financial statement, including assets, liabilities and debts, and transactions; or data in a credit or "consumer report" (as defined under 15 U.S.C. § 1681a).

With respect to the definition of the term *sensitive personal data*, the Department of Justice is considering or further defining categorical exclusions to the extent that data consists of:

i. public or nonpublic data that does not relate to an individual, including such data that meets the definition of a "trade secret" (as defined in 18

U.S.C. § 1839(3)) or "proprietary information" (as defined in 50 U.S.C. § 1708(d)(7));

ii. data that is lawfully available to the public from a Federal, State, or local government record or in widely distributed media (such as court records or other sources that are generally available to the public through unrestricted and open-access repositories);

iii. personal communications that do not transfer anything of value (*see* 50 U.S.C. § 1702(b)(1)); or

iv. *information or informational materials* (*see* 50 U.S.C. § 1702(b)(3)), which would be defined further in the regulations. The Department of Justice anticipates interpreting the phrase "*information or informational materials*" as including expressive information, like videos and artwork, and excluding non-expressive data, consistent with the speech-protective purpose of 50 U.S.C. § 1702(b)(3).

Bulk thresholds. The program would establish volume-based thresholds for each category of *sensitive personal data* and for combined datasets. The Department of Justice is considering the following approach to determine the bulk thresholds.

To the maximum extent feasible, the bulk thresholds would be set based on a risk-based assessment that examines threat, vulnerabilities, and consequences as components of risk. In the context of the bulk thresholds, a risk-based assessment would account for the characteristics of datasets that affect the data's vulnerability to exploitation by countries of concern and that affect the consequences of exploitation. These characteristics may include both human-centric characteristics (which describe a data set in terms of its potential value to a human analyst) and machine-centric characteristics (which describe how easily a data set could be processed by a computer system). The framework's human-centric characteristics may include how many individuals a data set covers (size), how the data could be used (purpose), how easy it is to deliberately change the data (changeability), who tracks and manages the data (control), and how easy the data is to obtain (availability). The framework's machine-centric characteristics may

include the number of data points in a dataset (volume), how quickly the dataset evolves (velocity), how specifically a data set targets a sensitive group (correlation), and how much processing is required to use the data (quality). Applying this style of framework would allow for a particularized assessment of the relative sensitivity of each of the six categories of *sensitive personal data* and would inform the volume threshold applicable to each category.

Based on a preliminary risk assessment, the Department of Justice, in consultation with other agencies, is considering adopting bulk thresholds within the following ranges, and would welcome additional analysis about the costs and benefits of specific thresholds for each category:

	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 *biometric 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 1,000 *U.S. persons*	More than 10,000 *U.S. persons* (for *biometric 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*

The Department of Justice proposes to operationalize these bulk thresholds as follows:

> The term *bulk U.S. sensitive personal data* means a collection or set of data relating to *U.S. persons*, in any format, regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted and that includes, at any point in the preceding twelve months, whether through a single *covered data transaction* or aggregated across *covered data transactions* involving the same *foreign person* or *covered person*:
>
> (i) *human genomic data* collected or maintained on more than [number of] *U.S. persons*;

(ii) *biometric identifiers* collected or maintained on more than [number of] *U.S. persons*;

(iii) *precise geolocation data* collected or maintained on more than [number of] *U.S. devices*;

(iv) *personal health data* collected or maintained on more than [number of] *U.S. persons*;

(v) *personal financial data* collected or maintained on more than [number of] *U.S. persons*;

(vi) *covered personal identifiers* collected or maintained on more than [number of] *U.S. persons*; or

(vii) *combined data*, meaning any collection or set of data that contains more than one of categories (i) through (vi), or that contains any *listed identifier* linked to categories (i) through (v), that meets the threshold number of persons or devices collected or maintained in the aggregate for the lowest number of *U.S. persons* or *U.S. devices* in any category of data present.

The ANPRM seeks comment on this topic, including:

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?
2. Should the Department of Justice treat data that is anonymized, pseudonymized, de-identified, or encrypted differently? If so, why?
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?
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.
5. The Executive Order directs a report and recommendation assessing the

risks and benefits of regulating transactions involving other specified types of human 'omic data. Should data *transactions* involving these other types of human 'omic data be regulated? If so, which types of human 'omic data? What risks, scientific value, and economic costs should be considered?

6. What, if any, possible unintended consequences could result from the definition (including the bulk thresholds) under consideration? In particular, to what extent would the approach contemplated here affect individuals' rights to share their own biospecimens and health, genomic, and other data?

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?

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*?

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 § 1798.140(w)) or a radius of 1,750 feet (*see, e.g.*, Utah Civ. Code § 13-61-101(33(a)))?

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?

12. How do businesses use each category of *sensitive personal data*, particularly in the cross-border context, and how would the ranges of bulk thresholds under consideration affect businesses' ability to engage in data *transactions* with *countries of concern* or *covered persons*?

13. Should the classes of *listed identifiers*, such as for government identification numbers and financial account numbers, include truncated versions of the

full numbers? If so, how should "truncated" be defined?

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?

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"?

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?

C. Government-Related Data

In addition to authorizing the Attorney General to address the national-security risks posed by transactions involving bulk sensitive personal data, the Order also authorizes the Attorney General to prohibit or otherwise restrict U.S. persons from

engaging in certain transactions involving government-related data regardless of volume.

The Order defines the term "United States Government-related data" as:

> "sensitive personal data that, regardless of volume, the Attorney General determines poses a heightened risk of being exploited by a country of concern to harm United States national security and that:
>
> (i) a transacting party identifies as being linked or linkable to categories of current or recent former employees or contractors, or former senior officials, of the Federal Government, including the military, as specified in regulations issued by the Attorney General pursuant to section 2 of th[e] order;
>
> (ii) is linked to categories of data that could be used to identify current or recent former employees or contractors, or former senior officials, of the Federal Government, including the military, as specified in regulations issued by the Attorney General pursuant to section 2 of th[e] order; or
>
> (iii) is linked or linkable to certain sensitive locations, the geographical areas of which will be specified publicly, that are controlled by the Federal Government, including the military."

The Department of Justice is considering further defining the term *government-related data* to include two data categories: (1) any *precise geolocation data*, regardless of volume, for any location within any area enumerated on a list of specific geofenced areas associated with military, other government, or other sensitive facilities or locations (the *Government-Related Location Data List*), or (2) any *sensitive personal data*, regardless of volume, that a transacting party markets as linked or linkable to current or recent former employees or contractors, or former senior officials, of the U.S. government, including the military and Intelligence Community.

With respect to the location subcategory, the *Government-Related Location Data List* would be created through an interagency process in which each agency identifies any geofenced areas relative to its equities for inclusion on the list, and DOJ would maintain and publish the list.

The Department of Justice currently intends the personnel subcategory to apply to scenarios such as the following:

- *Example 10.* A U.S. company advertises the sale of a set of *sensitive personal data* as belonging to "active duty" personnel, "military personnel who like to read," "DoD" personnel, "government employees," or "communities that are heavily connected to a nearby military base."

- *Example 11.* In discussing the sale of a set of *sensitive personal data* with a foreign counterparty, a U.S. company describes the data set as belonging to members of a specific organization, which restricts membership to current and former members of the military and their families.

The ANPRM seeks comment on this topic, including:

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"?

18. Are there categories of *government-related data* that should be added to the definition? Are there categories proposed that should be removed? Please explain.

19. How should the Department of Justice define data that is "marketed as linked or linkable" to current or recent former employees or contractors, or former senior officials, of the U.S. Government (including the military or Intelligence Community)? What are the current industry practices?

20. How would the contemplated definitions of *bulk sensitive personal data* and *government-related data* affect health and related research activities, such as genomic research on deceased U.S. persons who were former senior U.S. officials or recent former employees or contractors? To what extent do such activities involve *covered data transactions* with *countries of concern* or *covered persons* that would be prohibited or regulated under this program?

Should the Department of Justice consider a general license for such activities, and if so, what should the parameters be for such a license?

21. What, if any, possible unintended consequences could result from the definition of *government-related data* under consideration?

D. Covered Data Transactions

The Order authorizes the Attorney General to prohibit or otherwise restrict United States persons from engaging in transactions meeting several criteria and requires the Attorney General to identify classes of transactions subject to those prohibitions or restrictions. With respect to defining what would constitute a *covered data transaction*, the Department of Justice proposes to carefully tailor the program to achieve the Order's intent and effect. Consequently, the Department of Justice is considering adopting the following definitions relevant to the concept of a *covered data transaction*:

> A *transaction* is any acquisition, holding, use, transfer, transportation, exportation of, or dealing in any property in which a foreign country or national thereof has an interest.
>
> A *covered data transaction* is any *transaction* that involves any *bulk U.S. sensitive personal data* or *government-related data* and that involves: (1) *data brokerage*; (2) a *vendor agreement*; (3) an *employment agreement*; or (4) an *investment agreement*.

Under this definition of *covered data transactions* and the definition of *access* below (which includes both actual, as well as "the ability to" exercise, physical or logical access), prohibited *transactions* would be those *covered data transactions* that are categorically determined to pose an unacceptable risk to national security because they may enable *countries of concern* or *covered persons* to *access bulk U.S. sensitive personal data* or *government-related data*. Likewise, under these definitions, restricted *transactions* would be those *covered data transactions* that are categorically determined

to pose an unacceptable risk to national security because they may enable *countries of concern* or *covered persons* to *access bulk U.S. sensitive personal data* or *government-related data* unless the *security requirements* are implemented. The program would take a categorical approach to regulating *covered data transactions*; it would not rely on transacting parties or the government to determine whether specific *covered data transactions* within the classes of prohibited and restricted *transactions* individually pose unacceptable risks of *access*.

Basic terms. The Department of Justice is considering defining the term *access* to mean "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." The Department of Justice is considering defining the term *U.S. device* to mean "any device that is linked or linkable to a *U.S. person*." The Department of Justice is also considering defining the terms *entity*, *foreign person*, *person*, and *U.S. person* as follows, consistent with the definitions of those terms in other IEEPA-based regulations, including those contained in relevant sections of Title 31 of the Code of Federal Regulations:

> The term *entity* means a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization.
>
> The term *foreign person* means any person that is not a *U.S. person*. (For clarity, a foreign branch of a U.S. company would generally be treated the same as the U.S. company itself—as a *U.S. person*, not a *foreign person*.)
>
> The term *person* means an individual or *entity*.
>
> The term *U.S. person* means any United States citizen, national, or lawful permanent resident; or any individual admitted to the United States as a refugee under 8 U.S.C. § 1157 or granted asylum under 8 U.S.C. § 1158; or any *entity*

organized solely under the laws of the United States or any jurisdiction within the United States (including foreign branches); or any *person* in the United States.

- *Example 12.* An individual is a citizen of a *country of concern* and is in the United States. The individual is a *U.S. person.*
- *Example 13.* An individual is a U.S. citizen. The individual is a *U.S. person*, regardless of location.
- *Example 14.* An individual is a dual citizen of the United States and a *country of concern*. The individual is a *U.S. person*, regardless of location.
- *Example 15.* An individual is a citizen of a *country of concern*, is not a permanent resident alien of the United States, and is outside the United States. The individual is a *foreign person.*

Data brokerage. The program would define *data brokerage* as the sale of, licensing of *access* to, or similar commercial *transactions* involving the transfer of data from any *person* (the provider) to any other *person* (the recipient), where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data. The Department of Justice currently intends *data brokerage* to apply to scenarios such as the following:

- *Example 16.* A U.S. company sells *bulk U.S. sensitive personal data* to an *entity* headquartered in a *country of concern.*
- *Example 17.* A U.S. company enters into an agreement that gives a *covered person* a license to *access government-related data* held by the U.S. company.
- *Example 18.* A U.S. organization maintains a database of *bulk U.S. sensitive personal data* and offers annual memberships for a fee that provide members a license to *access* that data. Providing an annual membership to a *covered person* would constitute a prohibited *data brokerage*.

Vendor agreement. The contemplated program would define a *vendor agreement* as any agreement or arrangement, other than an *employment agreement*, in which any *person* provides goods or services to another *person*, including *cloud-computing services*,

in exchange for payment or other consideration. *Cloud-computing services* would be defined as services related to the provision or use of "cloud computing," including "Infrastructure-as-a-Service (IaaS)," "Platform-as-a-Service (PaaS)," and "Software-as-a-Service (SaaS)" (as those terms are defined in NIST Special Publication 800-145). The Department of Justice currently intends *vendor agreements* to apply to scenarios such as the following:

- *Example 19.* A U.S. company collects bulk *precise geolocation data* from U.S. users through an app. The U.S. company enters into an agreement with a company headquartered in a *country of concern* to process and store this data.

- *Example 20.* A medical facility in the United States contracts with a company headquartered in a *country of concern* to provide IT-related services. The medical facility has bulk *personal health data* on its U.S. patients. The IT services provided under the contract involve *access* to the medical facility's systems containing the bulk *personal health data.*

- *Example 21.* A U.S. company, which is owned by an entity headquartered in a *country of concern* and has been designated a *covered person,* establishes a new data center in the United States to offer managed services. The U.S. company's data center serves as a vendor to various U.S. companies to store *bulk U.S. sensitive personal data* collected by those companies.

- *Example 22.* A U.S. company develops mobile games that collect bulk *precise geolocation data* and *biometric identifiers* of U.S. person users. The U.S. company contracts part of the software development to a *foreign person* who is primarily resident in a *country of concern* and is a *covered person.* The software-development services provided by the *covered person* under the contract involve *access* to the bulk *precise geolocation data* and *biometric identifiers.*

By contrast, the Department of Justice currently does not intend this category to apply to scenarios such as the following:

- *Example 23.* A U.S. multinational company maintains *bulk U.S. sensitive personal data* of *U.S. persons.* This company has a foreign branch, located in a *country of concern,* that has *access* to this data. The foreign branch contracts with a local company located in the *country of concern* to provide cleaning services for the foreign branch's facilities. Although the

foreign branch is a *U.S. person*, the local company is a *covered person*, and the contract is a *vendor agreement*, the services performed under this contract do not "involve" the *bulk U.S. sensitive personal data* and thus would not be a *covered data transaction* subject to regulation.

Employment agreement. The program would define an *employment agreement* as any agreement or arrangement in which an individual, other than as an independent contractor, performs work or performs job functions directly for a *person* in exchange for payment or other consideration, including employment on a board or committee, executive-level arrangements or services, and employment services at an operational level. The Department of Justice currently intends *employment agreements* to apply to scenarios such as the following:

- *Example 24.* A U.S. company that conducts consumer genomic testing collects and maintains bulk *human genomic data* from U.S. consumers. The U.S. company has global IT operations, including employing a team of individuals that are citizens of and primarily reside in a *country of concern* to provide back-end services. Employment as part of the global IT operations team includes *access* to the U.S. company's systems containing the bulk *human genomic data*.

- *Example 25.* A U.S. company develops its own mobile games and social media apps that collect the *bulk U.S. sensitive personal data* of its U.S. users. The U.S. company distributes these games and apps in the United States through U.S.-based digital distribution platforms for software applications. Although the U.S. company's development team does not employ any *covered persons*, the U.S. company intends to hire as CEO an individual designated by the Attorney General as a *covered person* because of evidence the CEO acts on behalf of a country of concern. The individual's authorities and responsibilities as CEO involve *access* to all data collected by the apps, including the *bulk U.S. sensitive personal data*.

- *Example 26.* A U.S. company has amassed *U.S persons'* bulk *sensitive personal data* by scraping public photos from social-media platforms and then enrolls those photos in a database of bulk *biometric identifiers* developed by the U.S. company, including face-data scans, for the purpose of training or enhancing facial-recognition software. The U.S. company intends to hire a *foreign person*, who primarily resides in a *country of concern*, as a project manager responsible for the database. The individual's employment as the lead project manager would involve *access* to the bulk *biometric identifiers*. The *employment agreement* would

be a *covered data transaction*.

- *Example 27.* A U.S. financial-services company seeks to hire a data scientist who is a citizen of a *country of concern* who primarily resides in that *country of concern* and who is developing a new AI-based personal assistant that could be sold as a standalone product to the company's customers. As part of that individual's employment, the data scientist would have administrator rights that allow that individual to access, download, and transmit bulk quantities of *personal financial data* not "ordinarily incident to and part of" the company's underlying provision of financial services to its customers.

Investment agreement. The program would define an *investment agreement* as any agreement or arrangement in which any *person*, in exchange for payment or other consideration, obtains direct or indirect ownership interests in or rights in relation to (1) real estate located in the United States or (2) a U.S. legal *entity*. The Department of Justice currently intends *investment agreements* to apply to scenarios such as the following:

- *Example 28.* A U.S. company intends to build a data center located in a U.S. territory. The data center will store bulk *personal health data* on *U.S. persons*. A foreign private-equity fund located in a *country of concern* agrees to provide capital for the construction of the data center in exchange for acquiring a majority ownership stake in the data center.

- *Example 29.* A foreign technology company subject to the jurisdiction of a *country of concern* and that the Attorney General has designated as a *covered person* enters into a shareholders' agreement with a U.S. business that develops mobile games and social media apps, acquiring a minority equity stake in the U.S. business. These games and apps systematically collect *bulk U.S. sensitive personal data* of its U.S. users. The *investment agreement* explicitly gives the foreign technology company the ability to *access* this data.

- *Example 30.* Same as Example 29, but the *investment agreement* either does not explicitly give the foreign technology company the right to *access* the data or explicitly forbids that access. The *investment agreement* 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*; whether the specific *investment agreement* poses a risk of *access* does not affect whether the

agreement is restricted.

By contrast, the Department of Justice does not intend to restrict *investment agreements* in scenarios such as the following:

- *Example 31.* Same as Example 29, but the U.S. business does not maintain or have access to any *bulk U.S. sensitive personal data* or *government-related data* (e.g., a pre-commercial company or start-up company). Because the data *transaction* does not involve any *bulk U.S. sensitive personal data* or *government-related data*, this *investment agreement* does not meet the definition of *covered data transaction.*

The Department of Justice is considering categorically excluding certain passive investments that do not convey the ownership interest or rights (including those that provide meaningful influence that could be used to obtain such access) that ordinarily pose an unacceptable risk to national security because they may give *countries of concern* or *covered persons access* to *bulk sensitive personal data* or *government-related data.* Specifically, the Department of Justice is considering categorically excluding, from the definition of *investment agreement*, any investment that:

(1) is made:

(a) into a publicly traded security, with "security" defined in section 3(a)(10) of the Securities Exchange Act of 1934, Public Law 73–291 (as codified as amended at 15 U.S.C. § 78c(a)(10)), denominated in any currency that trades on a securities exchange or through the method of trading that is commonly referred to as "over-the-counter," in any jurisdiction;

(b) into an index fund, mutual fund, exchange-traded fund, or a similar instrument (including associated derivatives) offered by an "investment company" (as defined in section 3(a)(1) of the Investment Company Act of 1940, Public Law 76-768, as codified as amended at 15 U.S.C. § 80a-3(a)(1)) or by a private investment fund; or

(c) as a limited partner into a venture capital fund, private equity fund, fund of funds, or other pooled investment fund, if the limited partner's contribution is solely capital into a limited partnership structure or equivalent and the limited partner cannot make managerial decisions, is not responsible for any debts beyond its investment, and does not have the

formal or informal ability to influence or participate in the fund's or a *U.S. person's* decision-making or operations;

(2) gives the *covered person* less than [a de minimis threshold] in total voting and equity interest in a *U.S. person*; and

(3) does not give a *covered person* rights beyond those reasonably considered to be standard minority shareholder protections, including (a) membership or observer rights on, or the right to nominate an individual to a position on, the board of directors or an equivalent governing body of the *U.S. person*, or (b) any other involvement, beyond the voting of shares, in substantive business decisions, management, or strategy of the *U.S. person*.

Finally, the Department of Justice is considering how the program should address *investment agreements* that are "covered transactions" subject to the jurisdiction of the Committee on Foreign Investment in the United States (CFIUS) under section 721 of the Defense Production Act of 1950, Public Law 81-774, as codified as amended at 50 U.S.C. § 4565. This topic is discussed separately in the section on "Coordination with Other Regulatory Regimes."

The ANPRM seeks comment on this topic, including:

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*?

23. With respect to the exclusion from the definition of *investment agreements* for certain low-risk investments, what de minimis threshold of voting or equity interest should the Department of Justice consider establishing?

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

25. Are there any additional scenarios or types of data *transactions* that would

be helpful to identify whether or not they would be restricted?

E. Countries of Concern

The Order requires the Attorney General to identify countries of concern. The Order defines "country of concern" as any foreign government that, as determined by the Attorney General with the concurrence of the Secretaries of State and Commerce, "(1) has engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons, and (2) poses a significant risk of exploiting bulk U.S. sensitive personal data or United States Government-related data to the detriment of the national security of the United States or the security and safety of U.S. persons, as specified in regulations issued by the Attorney General pursuant to section 2 of th[e] order."

The Department of Justice is considering adopting the Order's definition of the term *country of concern* without elaboration or amendment. The Department of Commerce, in implementing Executive Order 13873—in which the President declared a national emergency stemming from foreign adversaries' ability to exploit information and communications and technology services to, among other things, engage in malicious cyber-enabled activities—identified the following countries as having engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of the United States: the People's Republic of China, along with the Special Administrative Region of Hong Kong and the Special Administrative Region of Macau; the Russian Federation; the Islamic Republic of Iran; the Democratic People's Republic of Korea; the Republic of Cuba; and the Bolivarian Republic of Venezuela. *See* 15 CFR 7.4. This Order expands the scope of the national

emergency declared by the President in Executive Order 13873. Accordingly, the Department of Justice is considering identifying the same countries as *countries of concern* under the Order, as will be explained further in the notice of proposed rulemaking.

The ANPRM seeks comment on this topic, including:

26. Should the Department of Justice further elaborate in any way on the definition of *country of concern* to provide greater clarity?

27. Are there other factors or considerations relating to the abilities of the proposed *countries of concern* to *access* and exploit *bulk sensitive personal data* or *government-related data* to engage in nefarious activities that the Department of Justice should take into account when determining whether to identify the same countries as *countries of concern*?

F. Covered Persons

The Order requires the Attorney General to identify classes of covered persons, as appropriate, for the purposes of the Order. "Covered person" is defined by the Order as "an entity owned by, controlled by, or subject to the jurisdiction or direction of a country of concern; a foreign person who is an employee or contractor of such an entity; a foreign person who is an employee or contractor of a country of concern; a foreign person who is primarily resident in the territorial jurisdiction of a country of concern; or any person designated by the Attorney General as 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 the Order or its implementing regulations.

The Department of Justice is considering an approach that would identify a *covered person* as a *person* that meets the definition either by (1) falling into one of the classes without having been individually designated by the Department of Justice or (2) having been individually designated by the Department of Justice on a public list maintained and updated by the Department of Justice.

The Department of Justice is considering defining the term *covered person* as:

(1) an *entity* that is 50 percent or more owned, directly or indirectly, by a *country of concern*, or that is organized or chartered under the laws of, or has its principal place of business in, a *country of concern*;

(2) an *entity* that is 50 percent or more owned, directly or indirectly, by an *entity* described in category (1) or a *person* described in categories (3), (4), or (5);

(3) a *foreign person* who is an employee or contractor of a *country of concern* or of an *entity* described in categories (1), (2), or (5);

(4) a *foreign person* who is primarily resident in the territorial jurisdiction of a *country of concern*; or

(5) any *person* designated by the Attorney General as being owned or controlled by or subject to the jurisdiction or direction of a *country of concern*, or as acting on behalf of or purporting to act on behalf of a *country of concern* or *covered person*, or *knowingly* causing or *directing* a violation of these regulations.

Under this contemplated definition, citizens of *countries of concern* located in third countries (i.e., not located in the United States and not primarily resident in a *country of concern*) would not be categorically treated as *covered persons*. Instead, only a subset of *country-of-concern* citizens in third countries would qualify categorically as *covered persons*: those working for the government of a *country of concern* or for a covered entity (as described in category 3 above). All other *country-of-concern* citizens located in third countries would not qualify as *covered persons* except to the extent that

the Attorney General designates them. The term *covered person* would thus apply as follows to *country-of-concern* citizens:

- *Example 32. Foreign persons* primarily resident in Cuba, Iran or another *country of concern* would be categorically treated as *covered persons*.
- *Example 33.* Chinese or Russian citizens located in the United States would be treated as *U.S. persons* and would not be *covered persons* (except to the extent individually designated). They would be subject to the same prohibitions and restrictions as all other *U.S. persons* with respect to engaging in *covered data transactions* with *countries of concern* or *covered persons*.
- *Example 34.* Citizens of a *country of concern* who are primarily resident in a third country, such as Russian citizens primarily resident in the European Union or Cuban citizens primarily resident in South America, would not be *covered persons* except to the extent they are individually designated or to the extent that they are employees or contractors of a *country-of-concern* government or a covered entity.
- *Example 35.* A *foreign person* located abroad is employed by a company headquartered in the People's Republic of China. Because the *foreign person* is the employee of a covered entity, the person is a *covered person.*
- *Example 36.* A *foreign person* located abroad is employed by a company that has been designated as a *covered person.* Because the *foreign person* is the employee of a covered entity, the person is a *covered person.*

With respect to individually designated *covered persons*, the Department of Justice is considering maintaining a public list of persons determined to be *covered persons*, modeled on various sanctions designations lists maintained by OFAC. Inclusion on the Department of Justice's *covered person list* would have no effect on a person's inclusion on OFAC or other U.S. Government designation lists. As indicated by the contemplated definition of *covered person*, this list would identify "any *person* designated by the Attorney General as being owned or controlled by or subject to the jurisdiction or direction of a *country of concern*, or as acting on behalf of or purporting to act on behalf of a *country of concern* or *covered person*, or *knowingly* causing or

directing a violation of these regulations." This designations list would supplement the defined categories in the definition of *covered person* to provide direct and actual notice to regulated parties of specific designated persons, would inform the public regarding the specific designated persons subject to this regulation's requirements regarding prohibited and restricted *covered data transactions*, and would serve enforcement purposes. Importantly, however, the public list would not exhaustively include all *covered persons*, as any person that satisfies the criteria contained in the relevant definitions will be considered a *covered person* under the regulation, regardless of whether the person is identified on the public list.

The Department of Justice would establish a process to add to, remove from, or modify this list. The process would be similar to the internal processes used by other United States Government agencies that make designations based on IEEPA authorities, including interagency consultation to ensure that agencies with relevant equities and expertise may weigh in. For example, the Department of Justice would be free to consider, to the extent compliant with applicable law, any classified or unclassified information from any Federal agency or other source. A *person* would be able to seek administrative reconsideration of the Department of Justice's determination that they are a *covered person*, or assert that the circumstances resulting in the determination no longer apply, and thus seek to have the designation rescinded pursuant to applicable administrative procedures. This administrative appeals process would be based on, and substantially similar to, analogous programs maintained by other Federal agencies that exercise IEEPA authorities.

The ANPRM seeks comment on this topic, including:

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?

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?

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?

31. Other than certain lists maintained by OFAC and BIS, are there other designation lists accessible to industry that the Department of Justice should consider as a model for identifying potential *covered persons*?

32. How should the list be published? How should it be organized? In what format should the Department of Justice publish it?

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.

34. How quickly after a *covered person* is added to the list (or an existing listing

is modified) could industry take account of the new information in its compliance programs?

35. Are there specific sources that the Department of Justice should consult to identify potential candidates for designation? If so, which ones?

36. Should the Department of Justice maintain a public-facing channel for the public to report potential candidates for designation? Why or why not? If yes, who should be permitted to make such reports and what information should they be required to provide? Would it be preferrable that the information submitted be protected from public disclosure?

37. Are there any aspects of processes used by other Federal agencies for persons to request or petition for the removal or modification of a designation or listing that would be especially useful for this list? If so, which ones and why?

38. Are there any aspects of the IEEPA designations appeals processes maintained by other Federal agencies that are not necessary for this list? If so, which ones and why not?

G. Prohibitions

The Order specifically directs the Attorney General to promulgate regulations to prohibit or otherwise restrict United States persons from engaging in any acquisition, holding, use, transfer, transportation, or exportation of, or dealing in, any property in which a foreign country or national thereof has any interest ("transaction"), where the transaction:

i. involves bulk U.S. sensitive personal data or United States Government-related data, as further defined by regulations issued by the Attorney General;

ii. is a member of a class of transactions that has been determined by the Attorney General, in regulations issued by the Attorney General, to pose an unacceptable risk to the national security of the United States because the transactions may enable countries of concern or covered persons to access bulk U.S. sensitive personal data or United States Government-related data in a manner that contributes to the national emergency described in the Order;

iii. was initiated, is pending, or will be completed after the effective date of the regulations issued by the Attorney General;

iv. does not qualify for an exemption provided in, or is not authorized by a license issued pursuant to, the regulations issued by the Attorney General; and

v. is not, as defined in final rules implementing the Order, ordinarily incident to and part of the provision of financial services, including banking, capital markets, and financial insurance services, or required for compliance with any Federal statutory or regulatory requirements, including any regulations, guidance, or orders implementing those requirements.

The Order further requires the Attorney General to promulgate regulations that identify classes of transactions that meet the criteria specified above and are thus prohibited under the Order. The Order describes additional activities that are, or may be, prohibited. In particular, any conspiracy formed to violate the regulations and any action that has the purpose of evading, causes a violation of, or attempts to violate the Order or any regulation issued thereunder is prohibited. In addition, the Order provides authority to the Attorney General to prohibit U.S. persons from "knowingly directing transactions" that would be prohibited transactions pursuant to the Order if engaged in by a U.S. person. The Department of Justice may at a future date provide notices of proposed rulemaking to add classes of prohibited transactions.

For this ANPRM, the Department of Justice is considering the following five prohibitions for *covered data transactions*, which would become effective only upon the effective date of a final rule.

First, the program would contain a general prohibition that is subject to authorized exemptions. The program would be technology-agnostic and neutral as to the path or route that *bulk U.S. sensitive personal data* or *government-related data* travels:

> "Except as otherwise authorized pursuant to these regulations, no *U.S. person*, on or after the *effective date*, may knowingly engage in a *covered data transaction* with a *country of concern* or *covered person*."

The Department of Justice currently intends for the *knowingly* language in this and the other prohibitions to apply to persons who knew or should have known of the circumstances of the *transaction*. In its guidance on what an individual or entity "should have known" in such context, the Department proposes to take into account the relevant facts and circumstances, including the relative sophistication of the individual or entity at issue, the scale and sensitivity of the data involved, and the extent to which the parties to the *transaction* at issue appear to have been aware of and sought to evade the application of these rules. This is not intended to operate as a strict-liability standard. The *knowingly* language is also not intended to require *U.S. persons*, in engaging in *vendor agreements* and other classes of data *transactions* with *foreign persons*, to conduct due diligence on the employment practices of those *foreign persons* to determine whether they qualify as *covered persons*. But *persons* will be prohibited from evading or avoiding these prohibitions, including by knowingly structuring *transactions* in a manner that attempts to circumvent these prohibitions.

With respect to the *knowingly* language, the prohibitions would therefore not apply in scenarios such as the following:

- *Example 37.* A *U.S. person* engages in a *vendor* agreement *involving bulk sensitive personal data* with a *foreign person* who is not a *covered person.* The *foreign person* then employs an individual who is a *covered person* and grants them access to *bulk U.S. sensitive personal data* without the *U.S. person's* knowledge or direction. There is no *covered data transaction* between the *U.S. person* and the *covered person,* and there is no indication that the parties engaged in these *transactions* with the purpose of evading the regulations (such as the *U.S. person* having *knowingly directed* the *foreign person's employment agreement* with the *covered person* or the parties *knowingly* structuring a prohibited *covered data transaction* into these multiple *transactions* with the purpose of evading the prohibition).

- *Example 38.* A U.S. company sells DNA testing kits to U.S. consumers and maintains bulk *human genomic data* collected from those consumers. The U.S. company enters into a contract with a foreign cloud-computing company (which is not a *covered person*) to store the U.S. company's database of *human genomic data.* The foreign company hires employees from other countries, including citizens of *countries of concern* who primarily reside in a *country of concern,* to manage databases for its customers, including the U.S. company's human genomic database. There is no indication of evasion, such as the U.S. company *knowingly directing* the foreign company's *employment agreements* or the U.S. company *knowingly* engaging in and structuring these transactions to evade the regulations). The *cloud-computing services* agreement between the U.S. company and the foreign company would not be prohibited or restricted because that *covered data transaction* is between a *U.S. person* and a foreign company that does not meet the definition of a *covered person.* The *employment agreements* between the foreign company and the *covered persons* would not be prohibited or restricted because those agreements are between *foreign persons.*

By contrast, the prohibitions would apply in scenarios such as the following:

- *Example 39.* A U.S. subsidiary of a company headquartered in a *country of concern* collects *bulk precise geolocation data* from U.S. persons. The U.S. subsidiary is a *U.S. person,* and the parent company is a *covered person.* With the purpose of evading the regulations, the U.S. subsidiary enters into a *vendor agreement* with a foreign company that is not a *covered person,* which the U.S. subsidiary knows (or should know) is a shell company that subsequently outsources the *vendor agreement* to the U.S. subsidiary's parent company.

- *Example 40.* A U.S. company collects *bulk personal health data* from U.S. persons. With the purpose of evading the regulations, the U.S. company enters into a *vendor agreement* with a foreign company that is not a *covered person,* which the U.S. company knows (or should know) is a

shell company staffed entirely by *covered persons*.

Second, the contemplated program would include a prohibition specific to *data brokerage* to address *transactions* involving the onward transfer of *bulk U.S. sensitive personal data* or *government-related data* to *countries of concern* and *covered persons*. The Department of Justice is considering the following prohibition:

> "Except as otherwise authorized pursuant to these regulations, no *U.S. person*, on or after the *effective date*, may knowingly engage 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 *covered person*."

This narrow circumstance would be the only instance in which the contemplated program would regulate third-country *covered data transactions* (i.e., *U.S. persons*' *covered data transactions* in which a *country of concern* or *covered person* is not a party). The Department of Justice currently intends this prohibition to apply to scenarios such as the following:

- *Example 41.* A U.S. business *knowingly* enters into an agreement to sell bulk human genomic data to a European business that is not a *covered person*. The U.S. business is required to include in that agreement a limitation on the European business's right to resell that data to a *country of concern* or *covered person*.

Third, the contemplated program would include a prohibition to specifically address the risks posed by *covered data transactions* involving *access* by *countries of concern* to *U.S. persons*' bulk *human genomic data* and biospecimens from which that data can be derived—such as *covered data transactions* involving laboratories owned or operated by *covered persons*. The Department of Justice is considering the following prohibition:

> "Except as otherwise authorized pursuant to these regulations, no *U.S. person*, on or after the *effective date*, may knowingly engage in any *covered data transaction*

> with a *country of concern* or *covered person* that provides that *country of concern* or *covered person* with *access* to *bulk U.S. sensitive personal data* that consists of *human genomic data*, or to human biospecimens from which such data could be derived, on greater than [the applicable bulk threshold of] *U.S. persons* at any point in the preceding twelve months, whether in a single *covered data transaction* or aggregated across *covered data transactions*."

Fourth, as in other IEEPA-based regulations, the Department of Justice is considering rules that will also prohibit evasions, causing violations, attempts, and conspiracies.

Fifth, the Department of Justice is considering prohibiting *U.S. persons* from *knowingly directing* any *covered data transaction* that would be prohibited (including restricted transactions that do not comply with the *security requirements*) if engaged in by a *U.S. person*. For purposes of this provision, the Department of Justice is considering defining *knowingly* to mean that the *U.S. person* had actual knowledge of, or should have known about, the conduct, circumstance, or result. And the Department of Justice is considering defining *directing* to mean that a *U.S. person* has the authority (individually or as part of a group) to make decisions on behalf of a foreign entity, and exercises that authority to order, decide, or approve a *transaction* that would be prohibited under these regulations if engaged in by a *U.S. person*. The program will clarify that certain conduct that is attenuated from the risks to U.S. national security identified in the Order, such as the financing or underwriting of a *covered data transaction*, the processing, clearing, or sending of payments by a bank, and legal services, would not be covered as *directing* a *transaction* as defined by the regulations. This approach is narrower than the authority afforded to the Department of Justice under the Order.

The Department of Justice intends to use this authority to tailor the regulations to target the identified national-security threat by prohibiting *U.S.-person* activity such as:

- *Example 42.* A *U.S. person* is an officer, senior manager, or equivalent senior-level employee at a foreign company that is not a *covered person*,

and the foreign company undertakes a *covered data transaction* at that *U.S. person*'s direction or with that *U.S. person*'s approval when the *covered data transaction* would be prohibited if performed by a *U.S. person.*

- *Example 43.* Several *U.S. persons* launch, own, and operate a foreign company that is not a *covered person*, and that foreign company, under the *U.S. persons'* operation, undertakes *covered data transactions* that would be prohibited if performed by a *U.S. person.*

- *Example 44.* A *U.S. person* is employed at a U.S.-headquartered multinational company that has a foreign affiliate that is not a *covered person.* The *U.S. person* changes (or approves changes to) the operating policies and procedures of the foreign affiliate with the specific purpose of allowing the foreign affiliate to undertake *covered data transactions* that would be prohibited if performed by a *U.S. person.*

By contrast, the prohibition in the Order on *knowingly directing* transactions would not apply to scenarios such as the following:

- *Example 45.* A U.S. bank processes a payment from a *U.S. person* to a *covered person*, or from a *covered person* to a *U.S. person*, as part of that *U.S. person*'s engagement in a prohibited *data transaction.* The U.S. bank's activity would not be prohibited (although the *U.S. person*'s *covered data transaction* would be prohibited).

- *Example 46.* A U.S. financial institution underwrites a loan or otherwise provides financing for a foreign company that is not a *covered person*, and the foreign company undertakes *covered data transactions* that would be prohibited if performed by a *U.S. person.*

- *Example 47.* A *U.S. person*, who is employed at a foreign company that is not a *covered person*, signs paperwork approving the foreign company's procurement of real estate for its operations. The same foreign company separately conducts data *transactions* that use or are facilitated by operations at that real-estate location and that would be prohibited *covered data transactions* if performed by a *U.S. person*, but the U.S. employee has no role in approving or directing those separate data *transactions*.

- *Example 48.* A U.S. company owns or operates a submarine telecommunications cable with one landing point in a foreign country that is not a *country of concern* and one landing point in a *country of concern.* The U.S. company leases capacity on the cable to U.S. customers that transmit *bulk sensitive personal data* to the landing point in the *country of concern*, including transmissions as part of prohibited *covered data transactions*. The U.S. company's ownership or operation of the cable

would not be prohibited (although the U.S. customers' *covered data transactions* would be prohibited).

The ANPRM seeks comment on this topic, including:

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?
40. What modifications, if any, should be made to the proposed definitions above to enhance clarity?
41. What, if any, unintended consequences could result from the proposed definitions?
42. What, if any, alternate approaches should the Department of Justice consider to prevent the conduct in the *knowingly-directed* example scenarios described above?

H. Exempt Transactions

The Order recognizes that certain transactions will be exempt from any final rules. The Department of Justice is considering mirroring OFAC's approach in IEEPA-based sanctions regulations by explicitly identifying certain classes of data *transactions* that are exempt from the scope of its prohibitions and restrictions. As explained below, DOJ is considering exempting from this program: data *transactions* involving certain kinds of data; official business *transactions*; financial-services, payment-processing, and regulatory-compliance-related *transactions*; intra-entity *transactions* incident to business

operations; and *transactions* required or authorized by Federal law or international agreements.

Data transactions involving certain kinds of data. The program would exempt two classes of data *transactions* to the extent that they involve data that is statutorily exempt from regulation under IEEPA: *personal communications* (any postal, telegraphic, telephonic, or other personal communication that does not involve the transfer of anything of value, as set out under 50 U.S.C. § 1702(b)(1)) or *information* or *informational materials* (the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any *information or informational materials*, as set out under 50 U.S.C. § 1702(b)(3)) and as further interpreted and defined in the contemplated regulations).

Official business. The Order exempts "transactions for the conduct of the official business of the United States Government by employees, grantees, or contractors thereof, [and] transactions conducted pursuant to a grant, contract, or other agreement entered into with the United States Government." To implement this provision, the Department of Justice is considering exempting data *transactions* to the extent that they are for (1) the conduct of the official business of the United States Government by its employees, grantees, or contractors; (2) any authorized activity of any United States Government department or agency (including an activity that is performed by a Federal depository institution or credit union supervisory agency in the capacity of receiver or conservator); or (3) *transactions* conducted pursuant to a grant, contract, or other agreement entered into with the United States Government. Most notably, this exemption would exempt grantees and contactors of Federal departments and agencies, including the Department

of Health and Human Services, the Department of Veterans Affairs, the National Science Foundation, and the Department of Defense, so that those agencies can pursue grant-based and contract-based conditions to address risks that *countries of concern* can *access* sensitive personal data in *transactions* related to their agencies' own grants and contracts, as laid out in section 3(b) of the Order—without subjecting those grantees and contractors to dual regulation.

The Department of Justice proposes that this exemption would apply to, and thus exempt, scenarios such as the following:

- *Example 49.* A U.S. hospital receives a Federal grant to conduct research on *U.S. persons*. As part of that federally funded human genomic research, the U.S. hospital contracts with a foreign laboratory that is a *covered person*, hires a researcher that is a *covered person*, and gives the laboratory and researcher *access* to the human biospecimens and *human genomic data* in bulk. The contract with the foreign laboratory and the employment of the researcher would be prohibited *covered data transactions* if they were not part of the federally funded research.

Financial-services, payment-processing, and regulatory-compliance-related transactions. Section 2(a)(v) of the Order exempts any transaction that is, as defined by final rules implementing the Order, ordinarily incident to and part of the provision of financial services, including banking, capital markets, and financial insurance services, or required for compliance with any Federal statutory or regulatory requirements, including any regulations, guidance, or orders implementing those requirements. To further define this exemption, the Department of Justice is contemplating exempting data *transactions* to the extent that they are ordinarily incident to and part of the provision of financial services, including:

(i) banking, capital-markets, or financial-insurance services;

(ii) a financial activity authorized by 12 U.S.C. § 24 (Seventh) and rules and regulations thereunder;

(iii) an activity that is "financial in nature or incidental to a financial activity" or "complementary to a financial activity," as set forth in section 4(k) of the Bank Holding Company Act of 1956 and rules and regulations thereunder;

(iv) the provision or processing of payments involving the transfer of *personal financial data* or *covered personal identifiers* for the purchase and sale of goods and services (such as the purchase, sale, or transfer of consumer products and services through online shopping or e-commerce marketplaces), other than data *transactions* that involve *data brokerage*; and

(v) compliance with any Federal laws and regulations, including the Bank Secrecy Act, 12 U.S.C. §§ 1829b, 1951–1960, 31 U.S.C. §§ 310, 5311–5314, 5316–5336; the Securities Act of 1933, 15 U.S.C. §§ 77a et seq.; the Securities Exchange Act of 1934, 15 U.S.C. §§ 78a et seq.; the Investment Company Act of 1940, 15 U.S.C. §§ 80a-1 et seq.; the Investment Advisers Act of 1940, 15 U.S.C. §§ 80b-1 et seq.; the International Emergency Economic Powers Act, 50 U.S.C. §§ 1701 et seq.; the Export Administration Regulations, 15 CFR 730, et seq.; or any notes, guidance, orders, directives, or additional regulations related thereto.

The Department of Justice would consult the Department of the Treasury and other relevant agencies in interpreting and applying this exemption, including through guidance, advisory opinions, or licensing decisions.

The Department of Justice currently intends this exemption to apply to, and thus exempt, scenarios such as the following:

- *Example 50.* A U.S. company engages in a data *transaction* to transfer *personal financial data* in bulk to a financial institution that is incorporated in, located in, or subject to the jurisdiction or control of a *country of concern* to clear and settle electronic payment transactions between U.S. individuals and merchants in a *country of concern* where both the U.S. individuals and the merchants use the U.S. company's infrastructure, such as an e-commerce platform. Both the U.S. company's transaction transferring bulk *personal financial data* and the payment transactions by U.S. individuals are both exempt.

- *Example 51.* A U.S. bank or other financial institution engages in a data *transaction* with a *covered person* that is ordinarily incident to and part of ensuring complying with U.S. laws and regulations (such as OFAC sanctions and anti-money laundering programs required by the Bank Secrecy Act).

- *Example 52.* As ordinarily incident to and part of securitizing and selling

asset-backed obligations (such as mortgage and nonmortgage loans) to a *covered person*, a U.S. bank provides *bulk U.S. sensitive personal data* to the *covered person*.

- *Example 53.* A U.S. bank or other financial institution, as ordinarily incident to and part of facilitating payments to U.S. persons in a *country of concern*, stores and processes the customers' *bulk financial data* using a data center operated by a third-party service provider in the *country of concern*.

- *Example 54.* As part of operating an online marketplace for the purchase and sale of goods, a U.S. company, as ordinarily incident to and part of U.S. consumers' purchase of goods on that marketplace, transfers bulk contact information, payment information (e.g., credit-card account number, expiration data, and security code), and delivery address to a merchant in a *country of concern*.

Intra-entity transactions incident to business operations. The Department of Justice is considering exempting data *transactions* to the extent that they are (1) between a *U.S. person* and its subsidiary or affiliate located in (or otherwise subject to the ownership, direction, jurisdiction, or control) of a *country of concern*, and (2) ordinarily incident to and part of ancillary business operations (such as the sharing of employees' *covered personal identifiers* for human-resources purposes; payroll transactions like the payment of salaries and pension to overseas employees or contractors; paying business taxes or fees; purchasing business permits or licenses; sharing data with auditors and law firms for regulatory compliance; and risk-management purposes).

The Department of Justice currently intends this exemption to apply to, and thus exempt, scenarios such as the following:

- *Example 55.* A U.S company has a foreign subsidiary located in a *country of concern*, and the U.S. company's *U.S.-person* contractors perform services for the foreign subsidiary. As ordinarily incident to and part of the foreign subsidiary's payments to the *U.S.-person* contractors for those services, the U.S. company engages in a data *transaction* that gives the subsidiary *access* to the *U.S.-person* contractors' bulk *personal financial*

data and *covered personal identifiers*.

By contrast, the Department of Justice intends this exemption not to apply to scenarios such as the following:

- *Example 56.* A U.S. company aggregates bulk *personal financial data*. The U.S. company has a non-wholly owned subsidiary that is a *covered person* because it is headquartered in a *country of concern*. The subsidiary is subject to the *country of concern*'s national-security laws requiring it to cooperate with and assist the country's intelligence services. The exemption would not apply to the U.S. parent's grant of a license to the subsidiary to access the parent's databases containing the bulk *personal financial data* for the purpose of complying with a request or order by the *country of concern* under those national-security laws to provide access to that data.

Transactions required or authorized by Federal law or international agreements.

The Department of Justice is considering exempting data *transactions* to the extent that they are required or authorized by Federal law or pursuant to an international agreement (such as the exchange of passenger-manifest information, INTERPOL requests, and public-health surveillance).

The ANPRM seeks comment on this topic, including:

43. What modifications, if any, should be made to the proposed definitions above to enhance clarity?

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

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

I. Security Requirements for Restricted Transactions

As described above, the Department of Justice is considering identifying three classes of restricted *covered data transactions* (*vendor agreements*, *employment agreements*, and *investment agreements*) that would be otherwise prohibited unless they

meet certain conditions (*security requirements*) that mitigate the threats posed by *access* to the *bulk U.S. sensitive personal data* or *government-related data* by a *country of concern* or *covered person.* While the security requirements are still under development and will be available to the public at later date, the Department of Homeland Security, in coordination with the Department of Justice, has developed an outline of what the security requirements might entail, and that outline is previewed here only as context for the rest of the contemplated program and other topics on which questions are sought in this ANPRM.

The primary goal of the *security requirements* is to address national-security and foreign-policy threats that arise when *countries of concern* and *covered persons* can *access bulk U.S. sensitive personal data* or *government-related data* that may be implicated by the classes of restricted *covered data transactions*. The contemplated *security requirements* would be based on, as applicable and appropriate, existing performance goals, guidance, practices, and controls, such as the Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Performance Goals (CPG), National Institute of Standards & Technology (NIST) Cybersecurity Framework (CSF), NIST Privacy Framework (PF), and NIST SP 800-171 rev. 3 ("Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations"). The Department of Justice proposes to decline to regulate restricted *covered data transactions* until the applicable *security requirements* are published, available to the public, and become effective by incorporation into the final rule. The Department of Homeland Security, in coordination with the Department of Justice, has outlined the following approach to the *security requirements*.

A restricted *covered data transaction* would be permissible if the *U.S. person*:

(1) implements *Basic Organizational Cybersecurity Posture requirements*;

(2) conducts the *covered data transaction* in compliance with the following four conditions: (a) *data minimization and masking*; (b) use of *privacy-preserving technologies*; (c) development of information-technology systems to prevent unauthorized disclosure; and (d) implementation of *logical and physical access controls*; and

(3) satisfies certain compliance-related conditions, such as retaining an independent auditor to perform annual testing and auditing of the requirements in (1) and (2) above, for so long as the *U.S. person* relies on compliance with those conditions to conduct the restricted *covered data transaction.*

Basic Organizational Cybersecurity Posture requirements applicable to all restricted *covered data transactions* could include practices such as CISA CPG 1.A, 1.B. 1.E, 1.F, 1.I, 2.P, 2.S, 2.Q, 4.A, and 5.A; NIST PF ID.IM-P1, ID.IM-P2, ID.BE-P1, and CT.DM-P9; and NIST CSF PR.AT-4 and PR.AT-5. Required controls could include NIST SP 800-171 3.1.1, 3.1.5, 3.3.1, 3.3.2, 3.3.3, 3.9.1, 3.9.2, and 3.14.6.

Data minimization and masking strategies (e.g., tokenization) could be used to eliminate *bulk U.S. sensitive personal* data or *government-related data* from some organizational scope to which a *country of concern* or *covered person* would have *access*. Required practices could include NIST PF CT.PO-P2, CT.DM-P8, CT.DP-P1, and CT.DP-P2.

Privacy-preserving technologies (e.g., based on homomorphic encryption or traditional encryption) could be deployed to enable restricted *covered data transactions* to proceed without exposing the *bulk U.S. sensitive personal* data or *government-related data* itself to *countries of concern* and *covered persons*. Required practices could include CISA CPG 2.K and 2.L; NIST PF CT.DP-P1; and NST PF/CSF PR DS-P1 and PR DS-P2. Required controls could include NIST SP 800-181 3.13.8, 3.13.10, and 3.13.11, and ones analogous to the controls described in 15 CFR 734.18(a)(5).

Logical and physical access controls could include role-based *access* management, such as credentialed *access* to both data systems and physical facilities containing *bulk U.S. sensitive personal* data or *government-related data*. Required practices could include CISA CPG 2.B, 2.D, 2.F, 2.G, 2.H, 2.T, 2.U, and 2.V; and NIST PF/CSF PR.AC-P1, PR.AC-P2, PR.AC-P3, PR.AC-P4, PR.AC-P5, PR.AC-P6, and PR.AC-P7. Required controls could include NIST SP 800-171 3.1.2, 3.1.3, 3.1.8, 3.1.10, 3.1.11, 3.1.12, 3.5.1, 3.5.3, 3.5.5, 3.5.7, 3.10.1, 3.10.2, and 3.10.7.

Under the contemplated program, a restricted *covered data transaction* would become prohibited if the parties fail to comply with the *security requirements*.

The Department of Homeland Security will propose and solicit public comment on the *security requirements* through a separate process.

J. Licenses

The Order authorizes the Attorney General, in concurrence with the Departments of State, Commerce, and Homeland Security, and in consultation with other relevant agencies, to issue (including to modify or rescind) licenses authorizing *covered data transactions* that would otherwise be prohibited or restricted. The Department of Justice

is considering a license regime that would be modeled on the licensing regime used by OFAC and would incorporate both general and specific licenses. These licenses would approve, or impose conditions on, *covered data transactions* that are prohibited or restricted and would include an interagency consultation process to ensure that agencies with relevant equities and expertise may weigh in. The Department of Justice is considering this type of licensing regime because, among other reasons, it could give regulated parties the ability to bring specific concerns to the Department of Justice and seek appropriate regulatory relief. Licensing could also provide the Department of Justice with flexibility to resolve marginal, unique, or particularly sensitive cases, either generally or in individual matters.

General licenses. Under the regime that the Department of Justice is considering, the Attorney General could issue and publish general licenses authorizing, under appropriate terms and conditions, certain types of *covered data transactions* that are subject to the requirements contained in the rules. Persons availing themselves of certain general licenses may be required to file reports and statements in accordance with the instructions specified in those licenses. Failure to timely file all required information in such reports or statements may nullify the authorization otherwise provided by the general license and result in violations of the applicable prohibitions that may be subject to enforcement action. General licenses could also be used to ease industry's transition once the rules become effective by potentially, for example, authorizing orderly wind-down conditions for *covered data transactions* that would otherwise be prohibited by the rules.

Specific licenses. The Department of Justice is also considering whether, as part of the rulemaking, to impose certain requirements that would apply to all persons who receive specific licenses. Those requirements could include, for example: (1) an ongoing obligation to provide reports regarding the authorized *transactions*; or (2) a requirement that any *person* receiving a specific license to transact in *bulk U.S. sensitive personal data* or *government-related data* must, to the extent feasible, provide assurances that any data transferred pursuant to such *transactions* can be recovered, irretrievably deleted, or otherwise rendered non-functional. The Department of Justice is also considering requiring applicants for specific licenses to use forms and procedures published by the Department of Justice, and allowing applicants and any other party in interest to request reconsideration of the denial of a license based on new facts or changed circumstances. The ANPRM seeks comment on this topic, including:

46. Would general and specific licenses be useful to regulated parties? Why or why not?
47. Should any or all specific licenses be published, provided that such publication complies with applicable laws and regulations (e.g., regarding the protection of confidential business information)? If so, how should they be published? How could the publication of specific licenses assist or harm regulated parties?
48. How should the Department of Justice assess or evaluate the purported costs of complying with the conditions of a general license or a specific license? Are the costs of reporting on licensed *transactions*, auditing them, or ensuring that they can be rendered non-functional if noncompliant likely to

scale with *transaction* size? With data volume? Based on other factors?

49. What, if any, general licenses would be useful to assist in the industry's transition once the rules take effect? Why? Please be specific.

50. How should the Department of Justice assess time limitations on general licenses or specific licenses? For example, how should the Department of Justice calculate reasonable wind-down periods?

51. What factors should the Department of Justice assess when considering whether to grant or deny a specific license application?

52. Are there classes of data *transactions* that may become the subject of specific license applications that the Department of Justice should presumptively grant or presumptively deny? Why?

53. What is the technical feasibility of recovering, irretrievably deleting, or otherwise rendering non-functional data transferred pursuant to a licensed *covered data transaction*? What technical measures, solutions, or controls could be used for this purpose?

54. What forms or procedures should the Department of Justice consider when establishing the requirements for an application for a specific license?

55. Are there any aspects of the OFAC and BIS licensing processes that would be especially useful for this program? If so, which ones and why?

56. Are there any aspects of the OFAC and BIS licensing processes that would

not be useful for this program? If so, which ones and why not?

K. Interpretive Guidance

The Order requires the Attorney General to "establish, as appropriate, mechanisms to provide additional clarity to persons affected by th[e] order and any regulations implementing th[e] order."[12] The Department of Justice is currently considering creating a program to provide guidance in the form of written advisory opinions, similar to processes used by OFAC and BIS, and by the Department of Justice with respect to the Foreign Corrupt Practices Act (FCPA) and the Foreign Agents Registration Act (FARA). The Department of Justice is considering permitting any *U.S. person* engaging in *covered data transactions* regulated by the program to request an interpretation of any part of these regulations from the Attorney General. Examples of such requests could include guidance on (1) whether a particular *transaction* is a *covered data transaction* and whether it is prohibited or restricted; (2) whether the Attorney General would be likely to issue a license governing a particular data *transaction*; and (3) whether a *person* satisfies the definitions of these regulations (*e.g.*, *U.S. person*, *foreign person*, *covered person*). Consistent with other Federal advisory-opinion programs, the Department of Justice is considering requiring that advisory opinions may only be requested for actual—not hypothetical—data *transactions*, but need not involve only prospective conduct.

The Department of Justice is considering requiring requests for interpretive guidance to be made using forms and procedures published by the Department of Justice. These rules may include, for example: (1) a requirement that all requests must be made in

[12] With respect to the security requirements, the Secretary of Homeland Security, in coordination with the Attorney General, shall issue any interpretive guidance.

writing; (2) a requirement that all requests must identify all participants in the data *transaction* for which the opinion is being sought (i.e., a prohibition on anonymous requests); (3) a requirement that the requesting party cannot use the advisory opinion, or permit it to be used, as evidence that the United States Government determined that the data *transactions* described in the advisory opinion are compliant with any Federal or state law or regulation other than the rules; and (4) a requirement that advisory opinions may be requested only for actual, not hypothetical, conduct.

The Department of Justice is also considering whether to publish some or all advisory opinions once issued, provided that such publication complies with applicable laws and regulations (e.g., regarding the protection of confidential business information). Finally, in addition to advisory opinions addressing specific requests, the Department of Justice is considering the publication of more general interpretive guidance, such as Frequently Asked Questions.

The ANPRM seeks comment on this topic, including:

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?
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)?

60. If the Department of Justice decides to publish some or all advisory opinions, how should it do so?

61. How should the Department of Justice address circumstances in which an advisory opinion no longer applies (e.g., the relevant *country of concern* at the time the opinion was issued no longer meets the requirements for being a *country of concern*).

62. What forms or procedures should the Department of Justice consider when establishing the requirements for an acceptable advisory opinion request?

63. Are there additional models or other forms of interpretive guidance that the Department of Justice should consider? For example, should the Department of Justice be free to issue guidance even if no party has inquired about the relevant topic? Should these other forms of guidance be published? If so, how?

L. Compliance & Enforcement

The Order delegates to the Attorney General, in consultation with relevant agencies, the full extent of the authority vested in the President by IEEPA, and expressly states that the rules will "address the need for, as appropriate, recordkeeping and reporting of transactions to inform investigative, enforcement, and regulatory efforts." The Department of Justice wishes to achieve widespread compliance, and to gather the information necessary to administer and enforce the program, without unduly burdening *U.S. persons* or discouraging data *transactions* that the program is not intended to

address. Any enforcement guidance issued by the Department of Justice regarding the *security requirements* will be issued in coordination with the Department of Homeland Security.

Accordingly, the Department of Justice is currently considering creating and implementing a compliance and enforcement program modeled on the Department of the Treasury's IEEPA-based economic sanctions, which are administered by OFAC.

Due diligence and recordkeeping. With respect to due diligence and recordkeeping, the Department of Justice is considering a model in which *U.S. persons* subject to the contemplated program employ a risk-based approach to compliance by developing, implementing, and routinely updating a compliance program. The compliance program suitable for a particular *U.S. person* would be based on that *U.S. person*'s individualized risk profile and would vary depending on a variety of factors, including the *U.S. person*'s size and sophistication, products and services, customers and counterparties, and geographic locations. The Department of Justice is not proposing to prescribe general due-diligence or affirmative recordkeeping requirements on all *U.S. persons* engaged in *covered data transactions* with *foreign persons*. The Department of Justice is considering whether a *U.S. person*'s failure to develop an adequate due-diligence program would have consequences if that *U.S. person* violates the regulations, such as treating this failure as an aggravating factor in any enforcement action.

The Department of Justice is currently considering imposing affirmative due-diligence and recordkeeping requirements only as a condition of engaging in a restricted *covered data transaction* or as a condition of a general or specific license. This limited set of affirmative due-diligence and recordkeeping requirements would include "know your

vendor" and "know your customer" requirements. Consistent with OFAC's practice in IEEPA-based sanctions programs, the Department of Justice is considering requiring *U.S. persons* subject to the due-diligence requirements to keep records of their due diligence to assist in inspections and enforcement.

Reporting. Similarly, the Department of Justice is considering reporting requirements modeled on existing IEEPA-based reporting requirements. The contemplated program would not prescribe general reporting requirements for all *U.S. persons* engaged in data *transactions* with *foreign persons* (or even with all *covered persons*). Rather, the Department of Justice is considering requiring reporting only as conditions of certain categories of *U.S. persons* that are engaging in restricted *covered data transactions* or as conditions of a general or specific license, or in certain narrow circumstances to identify attempts to engage in prohibited *covered data transactions*. DOJ is considering these reporting requirements to help DOJ identify *covered data transactions* that are the highest priority for ongoing compliance and enforcement efforts. The categories of *U.S. persons* subject to affirmative reporting requirements could include:

- a *U.S. person* that (a) is 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*.

Likewise, the Department of Justice is considering requiring any person granted a license under the rules to provide annual certifications supported by available documentation that they have abided by the terms of any license granted.

Audits. To assist in ensuring compliance with the *security requirements* for restricted *covered data transactions* and with licenses issued pursuant to the rules, the Department of Justice is considering whether to require a *U.S. person* to comply with certain conditions in conducting a restricted *covered data transaction* (whether conducted pursuant to a license or not) or a prohibited *covered data transaction* pursuant to a license. These conditions may include (i) appointing an accredited auditor to annually assess compliance with and the effectiveness of the *security requirements* or conditions of the license, and (ii) delivering the results of the audit to the Department of Justice. The audit will need to address (i) the nature of the *U.S. person*'s *covered data transaction* and (ii) whether it is in accordance with applicable *security requirements,* the terms of any license issued by the Attorney General, or any other aspect of the regulations.

Investigation and enforcement. To assist in the investigation of potential noncompliance with the rules, the Department of Justice is considering requiring any *U.S. person* "to keep a full record of, and to furnish under oath, in the form of reports or otherwise," as may be required by the Attorney General, "complete information relative to" any *covered data transaction* subject to a prohibition or restriction. 50 U.S.C. § 1702(a)(2). For the avoidance of doubt, neither the Order nor its implementing regulations will create any new right of access by the U.S. Government to *U.S. persons'*

sensitive personal data or *government-related data*, or give the U.S. Government a new right to monitor *U.S. persons'* communications.

The Department of Justice is also considering establishing a process for imposing civil monetary penalties similar to the processes followed by OFAC and CFIUS, with mechanisms for pre-penalty notice, an opportunity to respond, and a final decision. Penalties could be based on noncompliance with the regulations, making material misstatements or omissions, making false certifications or submissions, or other actions or factors. The Department of Justice would, consistent with due-process requirements, give companies the relevant non-classified information that forms the basis of any enforcement action and a meaningful opportunity to respond.

The ANPRM seeks comment on this topic, including:

64. What additional guidance should the Department of Justice provide in describing what constitutes having "received and affirmatively rejected" a *covered data transaction* involving *data brokerage* for purposes of the reporting requirements?
65. Would reports about rejected *covered data transactions* involving *data brokerage* yield information that the Department of Justice could use to calibrate regulations, prioritize enforcement, and identify areas for further guidance in implementing the Order?
66. What new compliance and recordkeeping controls will *U.S. persons* anticipate needing to comply with the program as described in this ANPRM? To what extent would existing controls for compliance with other United States Government laws and regulations be useful for compliance

with this program? How could the Department of Justice reduce the paperwork burden of any new compliance requirements?

67. What additional information will *U.S. persons* need to collect for compliance purposes as a result of this program?

68. 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?

69. Is this due diligence already being done by *U.S. persons* in connection with *transactions* that would be *covered data transactions*—e.g., for other regulatory purposes, prudential purposes, or otherwise? If so, please explain. What, if any, third-party services are used to perform due diligence as it relates to *transactions* involving the *countries of concern* more generally?

70. What are the practicalities of complying with this obligation? What, if any, changes to the way that *U.S. persons* undertake due diligence would be required because of this standard? What might be the cost to *U.S. persons* of undertaking such due diligence? Please be specific.

71. For how long should the Department of Justice consider requiring entities to retain records that the rules require them to maintain?

72. Are there additional examples of high-priority data *transactions* that should be included in the reporting requirement? Should any of the examples given above be excluded?

73. What should the Department of Justice's role be in nominating, approving, or otherwise participating in the selection of an accredited auditor charged

with monitoring compliance with the *security requirements* or a license under the rules? What should the Department of Justice consider when reviewing a candidate to be an auditor under this provision? What types of service providers currently exist that could play this role?

74. How, if at all, should penalties and other enforcement mechanisms be tailored to the size, type, or sophistication of the *U.S. person* or to the nature of the violation?

75. What factors should the Department of Justice analyze when determining to impose a civil penalty, as well as the amount?

76. What, if any, additional procedural steps should the Department of Justice require as part of its process to impose penalties?

77. Other than noncompliance with the regulations, making material misstatements or omissions, and making false certifications or submissions, what other types of actions or factors should the Department of Justice consider as a predicate for a penalty?

78. What should the Department of Justice consider when deciding to issue a subpoena or other investigative demand pursuant to the rules?

79. Have limitations or complications arisen regarding the service of IEEPA-based subpoenas or investigative demands in the past under programs administered by other Federal agencies?

80. What transaction sources should the Department of Justice use to monitor

compliance with this program?

M. Coordination with Other Regulatory Regimes

The Order requires the Department of Justice to address, as appropriate, coordination with other United States Government entities, such as CFIUS, OFAC, BIS, and other entities implementing relevant programs, including those implementing Executive Order 13873 of May 15, 2019 (Securing the Information and Communications Technology and Services Supply Chain) and Executive Order 14034 of June 9, 2021 (Protecting Americans' Sensitive Data From Foreign Adversaries); and Executive Order 13913 of April 4, 2020 (Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector). The Department of Justice does not currently intend or anticipate that this program will have significant overlap with existing authorities. Existing authorities do not provide prospective, categorical rules to address the national-security risks posed by *transactions* between *U.S. persons* and *countries of concern* (or persons subject to their ownership, control, jurisdiction, or direction) that pose an unacceptable risk of providing those countries with *access* to *bulk U.S. sensitive personal data* or *government-related data.*

With respect to *investment agreements* between *U.S. persons* and *countries of concern* (or *covered persons*) that are also "covered transactions" subject to CFIUS review, *see generally* 50 U.S.C. § 4565, the Department of Justice is considering an approach in which this program would independently regulate, as restricted *covered data transactions*, *investment agreements* that are also "covered transactions" subject to review by CFIUS, unless and until CFIUS enters into or imposes mitigation measures to resolve national-security risk arising from a particular covered transaction (a "CFIUS

Action"). A CFIUS Action could take the form of, for example, a CFIUS interim order, a CFIUS determination to conclude action with respect to a covered transaction based on an order or mitigation agreement of data-security risks, or CFIUS's entry into a mitigation agreement governing the voluntary abandonment of the covered transaction. Once such a CFIUS Action occurs, the program proposed under this ANPRM would cease to apply to the particular *investment agreement* that constitutes the covered transaction subject to the CFIUS Action. This exemption in the regulations would apply categorically for all covered transactions that are subject to a CFIUS Action; the Department of Justice would not be required to issue a specific license for each *investment agreement* addressed by a CFIUS Action.

This approach would preserve CFIUS's authority to develop bespoke protections to mitigate risks arising from *investment agreements* that also qualify as CFIUS covered transactions—or recommend the President prohibit such a covered transaction—where CFIUS deems such action necessary to address national security risk arising from the covered transaction and would ensure that parties do not have overlapping obligations under more than one regulatory regime. To the extent that CFIUS identifies an unresolved national-security risk regarding access to sensitive personal data that arises from a particular covered transaction, the program's *security requirements* would set an important baseline for CFIUS to draw on in mitigating the unresolved risk, consistent with CFIUS's transaction-specific approach. Under this approach, a CFIUS Action would not be considered to have occurred where CFIUS has not reviewed a particular *investment agreement* or action concludes with respect to an *investment agreement* without any mitigation of data-security risks. In those instances, this program would

continue to independently regulate the *investment agreement* as a restricted *covered data transaction*. This approach allows this program to continue to address risks that may arise outside of CFIUS's reach, such as (1) risks associated with *investment agreements* that are not "covered transactions" and thus outside of CFIUS's authority (e.g., non-controlling investments involving sensitive personal data below CFIUS's one-million-person threshold or data that is not identifiable); (2) risks associated with "covered transactions" where the risk does not "arise[] as a result of the covered transaction," 50 U.S.C. § 4565(l)(3)(A)(i); and (3) risks that may arise in the temporal gap that occurs after parties enter into an *investment agreement* but before the particular covered transaction is filed with CFIUS and becomes subject to a CFIUS Action.

This proposed approach contemplates that CFIUS would retain its existing authority to enforce CFIUS Actions, and DOJ would retain the authority to enforce violations of obligations under the program. Since the program would no longer apply to a particular *covered data transaction* once a CFIUS Action has been taken, CFIUS and the data-security regulations would not create dual or overlapping obligations: Violations of the obligations under the data-security regulations could occur only before the occurrence of the CFIUS Action. DOJ would retain authority, at any time, to enforce any violations of obligations under the program that were committed while the program applied to the *covered data transaction*, even if the enforcement action occurs after a CFIUS Action has occurred. In such instances, DOJ would coordinate with CFIUS.

Regardless of the manner in which the regulations address *investment agreements*, the program's other rules for classes of *covered data transactions* would still apply. Even if the program proposed under this ANPRM ceased to apply to a particular *investment*

agreement subject to a CFIUS Action, *U.S. persons* would still have to comply with the program's rules for *covered data transactions* involving *data brokerage*, the provision of bulk *human genomic data* and human biospecimens, *vendor agreements*, *employment agreements*, and other *investment agreements* not subject to a CFIUS Action.

The ANPRM seeks comment on this topic, including:

81. How should the program address *investment agreements* that are also "covered transactions" subject to the jurisdiction of CFIUS? What are the pros and cons of the approach under consideration?
82. In terms of compliance, what are the considerations with the approach described above where this program would govern unless or until a CFIUS Action occurs?
83. What other potential overlaps or gaps, if any, may exist between the program contemplated here and existing authorities? How should this program address them? In particular, should the Department of Justice consider any adjustments to the program contemplated here in light of the consumer-reporting rulemaking under the Fair Credit Reporting Act that the Consumer Financial Protection Bureau is considering? *See* Final Report of the Small Business Review Panel on the CFPB's Proposals and Alternatives Under Consideration for the Consumer Reporting Rulemaking (Dec. 15, 2023), https://files.consumerfinance.gov/f/documents/cfpb_sbrefa-final-report_consumer-reporting-rulemaking_2024-01.pdf

[https://perma.cc/K75B-MKR3].

N. Economic Impact

The Department of Justice is committed to ensuring that the contemplated program is carefully scoped to the kinds of data *transactions* that present unacceptable national-security risks and minimizes unintended economic impacts. The Department of Justice currently anticipates that this program would have the following economic impacts.

For each of the two classes of prohibited *covered data transactions* (those involving *data brokerage* and those involving the provision of *human genomic data* or human biospecimens from which that data can be derived), the Department of Justice anticipates that the primary economic impacts will fall into two categories: (1) direct costs in the form of the lost economic value of the *covered data transactions* that are prohibited or forgone, and (2) indirect costs, such as the compliance costs to perform due diligence to ensure that transactions with *foreign persons* comply with the prohibitions. For each of the three classes of restricted *covered data transactions* (*vendor agreements*, *employment agreements*, and *investment agreements*), the Department of Justice anticipates that the primary economic impacts will fall into two categories: (1) direct costs in the form of the lost economic value of *covered data transactions* that are prohibited or forgone, and (2) indirect costs, such as the costs of complying with the *security requirements* to conduct restricted *covered data transactions* and with the reporting requirements.

Direct costs. As a preliminary matter, there does not appear to be a complete or reliable estimate of the markets for, or economic value of, each of these classes of

covered data transactions—especially at the level of granularity required to accurately account for the details of the contemplated program, such as the specific classes of prohibited and restricted *covered data transactions*, the *countries of concern*, the kinds of *sensitive personal data*, the classes of exempt *transactions* (such as financial-services *transactions*), and other carve-outs and definitions being considered for this program.

For example, with respect to *data brokerage*, estimates for the total global data broker market vary widely from around $50 billion to over $300 billion and do not appear to have clear or reliable methodologies whose validity can be easily assessed.[13] The United States is widely perceived as the largest market for *data brokerage*; for instance, major U.S. *data brokerage* firms report that a majority of their global revenues come from the domestic market and that Asia-Pacific revenues (which are not broken down further for markets for specific countries) account for approximately one to six percent of their global markets.[14] Likewise, although trade in services data from the U.S. Bureau of Economic Analysis (BEA) provides an alternative potential approach for identifying cross-border transactions in sensitive personal data, the BEA data is not

---

[13] *See, e.g.*, Catherine Tucker & Nico Neumann, *Buying Consumer Data? Tread Carefully*, Harvard Business Review (May 1, 2020), https://hbr.org/2020/05/buying-consumer-data-tread-carefully [https://perma.cc/GDY3-AWKQ]; OnAudience, *Global Data Market Size: 2017–2021* at 4, 8 (Nov. 2020), http://pressmania.pl/wp-content/uploads/2020/12/Global-Data-Market-Size-2017-2021-OnAudience-Report.pdf [https://perma.cc/7NQS-3TXK]; Knowledge Sourcing Intelligence, *Global Data Broker Market Size, Share, Opportunities, COVID-19 Impact, And Trends By Data Type (Consumer Data, Business Data), By End-User (BFSI, Retail, Automotive, Construction, Others), And By Geography – Forecasts from 2023 to 2028* (June 2023), https://www.knowledge-sourcing.com/report/global-data-broker-market [https://perma.cc/2ED8-WU9K]; Transparency Market Research, *Data Brokers Market* (July 2022), https://www.transparencymarketresearch.com/data-brokers-market.html [https://perma.cc/GL3M-MQMR]; Maximize Market Research, *Data Broker Market: Global Industry Analysis and Forecast (2024-2030)* (Jan. 2024), https://www.maximizemarketresearch.com/market-report/global-data-broker-market/55670/ [https://perma.cc/V2VJ-VX9A].

[14] *See, e.g.*, TransUnion, *TransUnion Announces Fourth Quarter 2022 Results* (Feb. 14, 2023), https://newsroom.transunion.com/transunion-announces-fourth-quarter-2022-results/ [https://perma.cc/S8QW-D8RS]; Experian, *Trading update, first quarter* (July 13, 2023), https://www.experianplc.com/content/dam/marketing/global/plc/en/assets/documents/results-and-presentations/2023/experian-q1-fy24-trading-update.pdf [https://perma.cc/3FCZ-U4CY].

measured in a way that allows any direct comparison to the program contemplated here. The BEA categories of "Database and Other Information Services" and "Telecommunications, Computer, and Other Information Services" appear to be the two closest. But those BEA categories are over-inclusive and under-inclusive relative to the categories of *covered data transactions* that would be prohibited or restricted under the contemplated program: These two BEA categories, for instance, include trade that would be outside the scope of the contemplated program, such as kinds of data (e.g., web-browser history) and activities (e.g., computer hardware, dissemination of data and databases like directories, mailing lists, and web-search portals, newspaper and periodical subscriptions, and library/archive services). Similarly, for instance, these two BEA categories exclude transactions that would be within the scope of the contemplated program, such as activity from advertising, trade in human genomic data, and exports by credit bureaus (which report their data exports separately under the broader heading of "Financial Services"). Nevertheless, as a point of comparison, the BEA data suggests that, in 2022, the United States exported $317 million in "Database and Other Information Services" to China and a combined $3.4 billion in "Telecommunications, Computer, and Other Information Services" to China and Hong Kong.

For restricted *covered data transactions*, the net direct lost economic value will also depend on the extent to which *U.S. persons* continue to pursue otherwise-prohibited *vendor agreements*, *employment agreements*, and *investment agreements* in compliance with the *security requirements*. Where *U.S. persons* determine not to pursue vendor, employment, or investment agreements with *covered persons*, the net cost will depend on the extent to which such agreements can be easily replaced with vendors, employers, and

investors that will not be subject to such restrictions. It is plausible, for example, that—faced with higher costs associated with executing a vendor agreement with a vendor based in a *country of concern*—a U.S. company will opt to drop its data-processing contract with that vendor and instead rely on a vendor based outside of a *country of concern*. Relative to the current status quo, this switch could represent a financial loss to the original U.S. company (which could now face a higher cost for data processing) while providing a net gain to the alternative data processing vendor. The opposite could also be true: that the relevant costs associated with complying with this program would not justify a U.S. business switching from a vendor based in a *country of concern* but instead would justify continuing with that vendor by implementing the security requirements.

We request economic data to further evaluate these direct costs.

Indirect costs. In addition to the direct costs of prohibited and restricted *covered data transactions*, U.S. companies that handle and transfer *bulk U.S. sensitive personal data* or *government-related data* may also incur costs to ensure that they are complying with the contemplated program. The universe of firms that transact in *bulk U.S. sensitive personal data* is larger than the subset of such firms that knowingly transfer such data to *countries of concern* or *covered persons*; this larger universe of firms will need to undertake some due-diligence measures to ensure their typical data transfers are not in fact going to *countries of concern* or *covered persons* (for prohibited *covered data transactions*) and to comply with the *security requirements* (for restricted *covered data transactions*). Such compliance costs will vary by sector and size of firm.

For prohibited *covered data transactions*, the costs of due diligence would likely vary significantly across companies, as with the costs of compliance for economic

sanctions, export controls, and other national-security and law-enforcement regulations. As explained above, the contemplated program would employ a risk-based approach, like sanctions and export controls, in which regulated *U.S. persons* implement compliance programs based on their individualized risk profiles. For example, in addition to complying with other aspects of the contemplated program, the upfront due-diligence compliance costs for companies with robust existing compliance programs (such as sanctions and export controls) may be lower, whereas other companies with less robust compliance programs or no existing compliance programs may incur greater costs. Any estimate of due-diligence compliance costs would benefit greatly from more robust information on the size of the industries for each of the classes of prohibited *covered data transactions*, per-company costs, and per-transaction costs.

Similarly, for restricted *covered data transactions*, the costs of complying with the *security requirements* will vary across U.S. companies depending on the level of cybersecurity maturity. At one end of the spectrum, many U.S. companies already have foundational baseline cybersecurity protocols and technology in place, and may face only the marginal cost of tailoring or re-deploying those existing protocols and technology against the particular *security requirements* contemplated here. At the other end of the spectrum, other U.S. companies with less mature cybersecurity programs may face greater costs to acquire and implement baseline cybersecurity protocols and technology. The overall costs to comply with the *security requirements* will depend on the number and distribution of U.S. companies within the markets for the classes of restricted *covered data transactions* with *countries of concern*. Economic reasoning suggests, however, that companies that choose to deploy security measures to conduct restricted

covered data transactions would not incur compliance costs that are greater than the revenue they could realize by implementing these measures.

For *U.S. persons* that do find they need to invest in additional due-diligence programs to ensure compliance with the *security requirements*, such spending may also create offsetting benefits in the form of lower risks of data breaches and cyber attacks. For example, a July 2023 study noted that the global average cost of a data breach was $4.45 million the previous year and a 15% increase over the previous three years.[15]

U.S. persons subject to the reporting requirements may also incur costs to comply with the reporting requirements—costs that may also vary by company depending on their individualized risk profile.

The net impact of these indirect costs appears difficult to measure accurately with available data. We request economic data to support measurement of these indirect costs.

The ANPRM seeks comment on this topic, including:

84. To what extent do the current markets for the classes of *covered data transactions* involve the categories of *sensitive personal data* contemplated here? What is the average estimated commercial value of these *covered data transactions*? What are reliable sources of information on the size, extent, and growth of the markets for each of the classes of prohibited and restricted *covered data transactions*?

85. What is the value of *covered data transactions* with *countries of concern*

[15] Industrial Cyber, *Data breach costs for critical infrastructure sector exceed $5 million, as time 'new currency' in cybersecurity* (July 25, 2023), https://industrialcyber.co/reports/data-breach-costs-for-critical-infrastructure-sector-exceed-5-million-as-time-new-currency-in-cybersecuritydata-breach-costs-for-critical-infrastructure-sector-exceed-5-million-as-time-new/ [https://perma.cc/9QDT-37CN].

that would be impacted by this regulation?

86. How many *covered data transactions* with *countries of concern* or *covered persons* that meet the bulk threshold requirements are typically conducted each year?

87. What are the economic sectors that will be expected to be impacted by the regulation? What is the average size, in both revenue and number of employees, of the firms impacted by the regulation? What is the expected impact per firm, as a percentage of overall revenue? What are the program's likely effects on existing jobs and new employment opportunities for affected firms and sectors?

88. What specific types of data are involved in *covered data transactions* that involve *data brokerage*? What is the general purpose of these transactions? How is this data stored? Is *U.S. persons*' data that is sold to customers in *countries of concern* stored on or retrieved from the same systems used to store or retrieve *U.S. persons*' data sold to customers outside the *countries of concern*? If not, what segmentation exists?

89. What kinds of best practices do *U.S. persons* engaged in *data brokerage* implement to screen potential customers in the *countries of concern* (or markets that present similar risk profiles)? How widely implemented are these best practices in the industry?

90. What is the estimated economic size of the *data brokerage* market? What are the best, most reliable sources of data for the size, extent, and growth rate of this market? What is the average value of a *covered data transaction*

involving *data brokerage*?

91. How can service providers be grouped in the third-party *data brokerage* market? What is the difference between a large, medium, and small broker? How consolidated is the market? What are key factors, business features or other models that providers use to differentiate themselves? To what degree are providers differentiated by features other than the size and scope of individual data sets?

92. What are the estimated sizes of the global *data brokerage* market for each of the six types of data identified in this contemplated regulation (i.e., *covered personal identifiers*, *personal financial data*, *precise geolocation data*, *personal health data*, *biometric identifiers*, *human genomic data*)? What is the estimated size of each of these markets in the United States and each of the identified *countries of concern*?

93. What is the estimated transaction volume for the *data brokerage* market (both first-party and third-party brokerage)? What percentage of these transactions involve one or more of the six categories of regulated *sensitive personal data*? What percentage of these transactions involves a *country of concern*?

94. How are transactions conducted in the *data brokerage* market? What percentage of the economic value of this market involves transfer of data? What percentage involves subscription *access* to centrally managed databases? What percentage involves analyzed or processed data? What

percentage involves *access* to raw, unprocessed data?

95. To what extent do *U.S. persons* engaged in *data brokerage* use any service providers in *countries of concern* connected to their brokerage activities—such as hiring outsourcing companies for cleaning and labeling datasets or signing agreements with cloud service providers to store datasets? What is the estimated economic value of these services?

96. How many firms will be impacted by the prohibition on the use of vendors from *countries of concern*? What will be the average cost per firm of switching from vendors subject to restrictions to vendors not subject to restrictions? Which sectors will they be in? What will be the average size of such a firm?

97. Are there any sectors, markets, or product or service categories where, after excluding restricted vendors, there is unlikely to be a sufficient number of firms available to supply the overall level of service required by the market?

98. What proportion and segments of the *cloud-computing services* market will be impacted by this regulation? What will be the specific impacts on the cloud infrastructure, platform, and services markets? What will be the impact on U.S. cloud computing companies seeking to do business in *countries of concern*?

99. What will be the impact on *cloud-computing service* companies based in *countries of concern*? Are there circumstances under which U.S. companies may still wish or be required to do business with *cloud-computing service* companies based in *countries of concern* after the implementation of this

regulation? In these circumstances, will U.S. companies still be able to conduct necessary business after the implementation of this regulation?

100. What will be the economic impact of prohibiting any *covered data transaction* that provides a *country of concern* or *covered person* with *access* to bulk U.S. *human genomic data* and human biospecimens from which that *sensitive personal data* can be derived, taking into account the proposed exemptions?

101. What sectors are involved in *access* to bulk U.S. *human genomic data* and human biospecimens? Are there any sectors that involve *access* to one, but not both, of these categories? What is the estimated size of these markets, as well as the overall volume and value of the *covered data transactions* involving this type of data?

102. What types of commercial transactions involve *human genomic data* and human biospecimens? Do any of these transactions involve exchange of the data? Do any of these transactions involve *access* to—but not exchange of—this sensitive personal data?

103. Is there sufficient commercial demand available outside *countries of concern* to replace demand lost as a result of the prohibition, and if so, where is such demand located? What is the timeline for pivoting to meet new demand?

104. What percentage of the U.S. workforce would be affected by the restrictions on *employment agreements*? How many firms will be impacted by this prohibition? Which sectors will they be in? What will be the average size of

such a firm?

105. What will be the major cost components of a regulatory compliance program? What will be the average cost of each of these components per firm? Which of these components will be flat cost, regardless of the size of firm? Which will have a variable, per-employee cost?

106. What is the estimated cost of implementing the *security requirements* contemplated in the regulation on a per-firm basis? What are the basic components of these costs? Which of these components are fixed, one-time costs? Which will be ongoing, recurring costs?

107. How could the Department of Justice mitigate the costs of compliance, particularly for small- and medium-sized enterprises? Are there measures that could be taken to reduce the economic impact of the regulatory regime without altering the fundamental scope or thresholds associated with the regulation?

108. Are there legitimate commercial reasons for a *covered person* to *access* data or information covered as part of the classes of restricted *covered data transactions*? To what degree will an inability to *access* this data affect that company's ability to provide goods or services to U.S. companies and individuals?

109. What would be the commercial impact on *U.S. persons* if *countries of concern* must conduct business in the United States without *access* to data covered by restricted *covered data transactions*? Are there other economic arrangements by which a company could obtain the benefits of the data

without directly *accessing* the data itself?

110. What additional costs and benefits should the Department of Justice consider, and how should they be estimated? Is there additional data on the economic costs and benefits that the Department of Justice should examine?

O. Overarching and Additional Inquiries

111. What additional example scenarios should the Department of Justice consider, evaluate, and address in a proposed rulemaking to provide clarity?

112. What time, if any, will *U.S. persons* that are currently engaged in the prohibited *covered data transactions* contemplated here need to wind-down those transactions? What time, if any, will *U.S. persons* that are currently engaged in the restricted *covered data transactions* contemplated here need to comply with the *security requirements* or else wind-down those transactions?

113. What costs would be incurred by maintaining the status quo (i.e., forgoing the contemplated regulations) with respect to any of the classes of prohibited and restricted *covered data transactions* under consideration?

114. Are there additional topics on which the Department of Justice should be seeking comment? If so, what are they and what is their relevance?

IV. Regulatory Certifications

This ANPRM has been drafted and reviewed in accordance with the Principles of Regulation in section 1(b) of Executive Order 12866 of September 30, 1993 (Regulatory Planning and Review), as amended by Executive Order 14094 of April 6, 2023 (Modernizing Regulatory Review), and in accordance with the General Principles of

Regulation in section 1(b) of Executive Order 13563 of January 18, 2011 (Improving Regulation and Regulatory Review). This ANPRM is a "significant" regulatory action pursuant to Executive Order 12866, as amended by Executive Order 14094 and, accordingly, has been reviewed by the Office of Information and Regulatory Affairs (OIRA) at the Office of Management and Budget (OMB). This action does not propose or impose any requirements; rather, this ANPRM is being published to seek information and comments from the public to inform the notice of proposed rulemaking required to implement the Order.

The requirements of the Regulatory Flexibility Act do not apply to this action because, at this stage, it is an ANPRM and not a "rule" as defined in 5 U.S.C. § 601.

Following review of the comments received in response to this ANPRM, the Department of Justice will conduct all relevant analyses as required by statute or Executive Order for the notice of proposed rulemaking required to implement the Order.

Dated: February 28, 2024

Matthew G. Olsen
Assistant Attorney General for National Security