Davis Polk

Biden administration proposes expanded limits on transfers of personal data to adversary countries

March 21, 2024 | Client Update | 18-minute read

A new proposal would require U.S. companies to comply with U.S. government cybersecurity standards before transferring bulk data to, or accepting investment from, companies based in targeted countries.

On February 28, 2024, President Biden issued Executive Order 14117, "Preventing Access to Americans' Bulk Sensitive Data and United States Government-Related Data by Countries of Concern" (the Order) pursuant to the International Emergency Economic Powers Act (IEEPA).[1] The Order directs DOJ and other relevant U.S. government agencies to develop a new regulatory framework "to restrict access by countries of concern to Americans' bulk sensitive personal data and United States Government-related data when such access would pose an unacceptable risk to the national security of the United States."[2]

Pursuant to the Order, DOJ concurrently issued an Advance Notice of Proposed Rulemaking (ANPRM) that outlines the core conceptual elements of a proposed framework intended to address what DOJ characterized as a "key gap in our national security authorities."[3] Key provisions of the ANPRM would require compliance with government cybersecurity standards before engaging in vendor or data brokering transactions involving bulk sensitive personal data and certain U.S. government-related data to entities and individuals based in (or controlled by persons based in) countries of concern, initially proposed to be China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba and Venezuela. Transfers of more sensitive data, notably genomic data, would be prohibited completely absent a specific license. Covered "sensitive" data types would include a substantial array of digital identifiers, geolocation data, biometric and health data, and personal financial data. Perhaps more significantly, the ANPRM would also condition or prohibit U.S. companies holding bulk sensitive data from accepting any investment (including noncontrolling investments, other than passive investment in publicly traded securities) from entities of concern. These restrictions apply even to transactions where the Committee on Foreign Investment in the United States would not have jurisdiction.

The Order and the ANPRM explicitly refrain from creating broad data onshoring or general data protection requirements and apply several layers of criteria to circumscribe covered data transactions. Furthermore, for the most part, the transactions that would initially be covered by the ANPRM would still be permitted so long as a sufficient data security program is in place.

Many details remain to be determined, and the rules may be expanded to cover broader categories of data and activity in the future. It is clear, though, that the Order and ANPRM build on previous actions by the Biden and Trump administrations to create an ambitious program to control access to data on U.S. persons by potential rivals, particularly China. The restrictions on use of China-based and Chinese-owned vendors and on acceptance of investment from countries of concern will create *de facto* regulation by the Department of Justice of cybersecurity standards for a broad range of U.S. companies.

This client update provides context on how these latest actions fit within the larger set of recent data protection measures and summarizes the key provisions of the Order and ANPRM. The 45-day public comment period on the ANPRM will conclude on April 15, 2024. The Order directs DOJ to publish a further Notice of Proposed Rulemaking (NPRM) by

August 26, 2024, at which point stakeholders will have another opportunity to comment on the more detailed rules implementing the proposed framework.

The context: related efforts to combat foreign actors' attempts to access U.S. data

The Order discusses the competing policy considerations underlying these proposals in some depth. The key threat contemplated is the use of sensitive personal data by countries of concern to track and build profiles on U.S. individuals, including federal employees and contractors. The Order notes that such profiles could be employed to blackmail or otherwise influence such individuals. They could also be used to intimidate political dissidents abroad and to limit freedom of expression. The Order stresses that even legitimate channels can provide sufficient data to enable these bad acts and that new technologies, such as AI, can link together seemingly disparate datasets or overcome anonymization techniques. Access can also be gained indirectly, such as via national security laws that require foreign firms to provide data to their home governments. On the other hand, the Order reiterates the United States' firm commitment to ensuring the free flow of information and an open internet and mandates that the Order be implemented consistent with these policy objectives.

Over the past several years the U.S. intelligence community has increasingly warned of efforts by foreign actors to engage in cyber espionage and attempts to access Americans' sensitive personal data. According to a recent intelligence analysis cited by the Order, China, Russia and other countries have built sophisticated capabilities to analyze and manipulate large quantities of personal information which can be used to influence or coerce Americans as well as activists and dissidents living in the United States. [4] Access to commercial datasets containing sensitive data through data brokers or ownership of U.S. companies that collect sensitive data can enable such activities.

A series of related efforts have emerged in response to this threat:

- **CFIUS review of noncontrolling foreign investments in businesses that collect sensitive personal data:** CFIUS has, since the Obama administration, increasingly been focusing on access to sensitive personal data of U.S. persons. This focus was formalized in the 2018 update of CFIUS's statutory authority, the Foreign Investment Risk Review Modernization Act (FIRRMA). FIRRMA and its implementing regulations made explicit CFIUS's practice by listing access to sensitive personal data as a potential national security threat arising from foreign acquisitions, making CFIUS notification mandatory for acquisitions of companies holding large quantities of sensitive personal data by state-owned actors, and expanding CFIUS's jurisdiction over certain noncontrolling investments.
- **ICTS review of foreign IT hardware and software**: In May 2019 President Trump issued Executive Order 13873, extended by President Biden's Executive Order 14034 in June 2021, giving the Commerce Department authority to prohibit the use of information and communications technology services (ICTS) designed, developed, manufactured, or supplied by foreign adversaries on national security grounds. The Commerce Department has issued rules permitting the Secretary of Commerce to call transactions in for review.
- **Federal government cybersecurity efforts:** Executive Order 14028 in May 2021 focused on coordinating and improving the federal government's cybersecurity efforts; however, it also leveraged the federal government's buying power by requiring improved cybersecurity in the supply chain for software to be sold to the federal government.

The new proposal is best seen as the latest step in efforts to develop a novel, interconnected and fairly extensive regulatory scheme to protect sensitive data, and we would expect the focus on data security as national security to continue and grow across agencies, authorities, and administrations.

Highlights from the DOJ's ANPRM

The DOJ's ANPRM addresses the core directive of the Order to develop a regulatory framework for controlling access to American's sensitive personal data by countries of concern. The ANPRM is not a binding final rule or even a fully developed proposed rule. Its provisions are broad and conceptual, raise many issues and questions for comment, and may shift significantly before more detailed rules are proposed. Care should be taken to avoid drawing overly strong conclusions about the shape of any final rule from the ANPRM.

The DOJ has proposed to issue rulemakings under Executive Order 14117 in tranches, based on priority. The current ANPRM is focused on those transactions that raise the highest national security risks. Additional rulemakings may follow.

At a high level, the ANPRM imposes a requirement to implement a data security program meeting to-be-developed federal standards before a U.S. person can enter into vendor, investment or employment agreements involving bulk sensitive personal data or government-related data with persons or entities in or controlled by countries of concern (in the case of investment agreements, whether or not the investor in fact has any access to the data). It also prohibits outright data brokerage transactions or transactions involving bulk genomic data with covered persons absent a license. The ANPRM contemplates a to-be-specified license program as well as the possible issuance of advisory opinions, but in general the proposed requirements are categorical and compliance is the responsibility of the affected parties; unlike CFIUS or the ICTS process, there is no case-by-case government review.

Scope

Covered data

The ANPRM defines two different types of data that would be covered by a proposed rule.

The first type of covered data is **bulk U.S. sensitive personal data**. The ANPRM defines “sensitive personal data” to include precise geolocation data, biometric identifiers, human genomic data, personal health data, and personal financial data. The term also encompasses “covered personal identifiers” – meaning a specific list of commonplace identifiers that includes government ID numbers such as Social Security Numbers, demographic data (such as name, birthdate, telephone number, or e-mail and street addresses), and advertising-related digital identifiers – that could be used to identify an individual from a data set or link data across multiple data sets to an individual. Not all datasets of personal identifiers would be covered. Standalone lists of personal identifiers not linked to other data would not be covered, nor would demographic data that is solely linked to other demographic data (such as a telephone directory). However, demographic data that is linked to another listed identifier, such as a list of first and last names linked to a list of advertising IDs, or to any other form of sensitive data, would be covered.

Restrictions on the data of private U.S. persons would only apply to transfers meeting bulk volume thresholds. In cases where data is combined the lowest threshold applicable to an involved data type would be used. The ANPRM has proposed possible ranges for the applicable thresholds. These are outlined in the following table.

Category:	Human genomic data	Biometrics identifiers	Precise geolocation data	Personal health data	Personal financial data	Covered personal identifiers
Proposed low threshold	> 100 U.S. persons	> 100 U.S. persons	> 100 U.S. devices	> 1,000 U.S. persons		> 10,000 U.S. persons
Proposed high threshold	> 1,000 U.S. persons	> 10,000 U.S. persons	> 10,000 U.S. devices	> 1 million U.S. persons		> 1 million U.S. persons

The second type of covered data is **government-related data**. This is defined at length in the ANPRM, but in broad strokes it is sensitive data that, regardless of volume, is determined by the Attorney General to pose a heightened risk of being exploited by a country of concern to harm national security and that could be used to identify government officials, employees and contractors or can be linked to sensitive locations. Any transaction involving government-related data would be covered regardless of volume.

Countries of concern and covered persons

Data transfer restrictions will apply to **countries of concern**,which will be identified by the Attorney General by regulation. The DOJ currently contemplates identifying China, Russia, Iran, North Korea, Cuba, and Venezuela as countries of concern.

Data transfer restrictions would also apply to transactions with **covered persons**, which are:

1. Any entity organized or having its principal place of business in a country of concern, or 50% or more owned by the government of a country of concern;
2. Any foreign person or entity primarily resident in the territory of a country of concern;
3. Any person or entity specifically designated by the DOJ as owned by, controlled by, or acting on behalf of a country of concern or other covered person;
4. Any entity 50% or more owned, directly or indirectly, by any of the foregoing; and
5. Any foreign person who is an employee or contractor of any of the foregoing.

A “foreign person” is any person or entity who is not (a) a U.S. citizen or permanent resident or (b) located in the United States. Essentially, companies and persons located in countries of concern, as well as companies outside those countries that they control and their respective employees and contractors, are covered. The Attorney General also has the power to designate U.S. (or foreign) persons as covered persons, in a process analogous to existing sanctions lists.

It is not entirely clear whether the ANPRM intends to cover U.S. entities owned by covered persons (read literally, the proposed definition appears to cover them, but the ANPRM states that it is not intended to apply to transactions between non-designated U.S. persons).

Types of transactions covered

The ANPRM applies to **covered data transactions**, which are four specified categories of transactions with covered persons involving bulk U.S. sensitive personal data or government-related data. Transaction is broadly defined as any acquisition, holding, use, transfer, transportation exportation of, or dealing in data in which a foreign country or national (from any jurisdiction) has an interest. The categories of covered data transactions are:

- **Data brokerage**, which is defined 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.
- **Vendor agreement**, which is any agreement or arrangement, other than an employment agreement, in which any person provides goods or services to another person for consideration, including cloud computing services.
- **Employment agreement**, which is 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.
- **Investment agreement**, which is 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 ANPRM clarifies by way of examples that **any investment agreement in a company that has access to bulk sensitive personal data or government-related data would be a covered data transaction even if the investment is noncontrolling and the foreign investor lacks access to the data**.
  - The ANPRM contemplates a possible exception for investments in publicly traded stock (that are fully passive and have no special governance rights) or through passive LP interests in an investment fund that is not a covered person. The exception is quite narrow, however, and direct private investment of any size, even without any governance rights, would be covered.

Persons required to comply

The ANPRM proposes rules applying to transactions between U.S. persons (citizens, permanent residents, entities organized solely under U.S. law, and persons and entities located in the United States) and foreign persons (all others). It does **not** apply to transactions between foreign persons, even if bulk sensitive personal data is involved. However, a U.S. person is prohibited from knowingly entering into a covered data transaction with any foreign person in order to evade the prohibitions or from directing the foreign person to engage in transactions with covered persons in relation to the bulk sensitive personal data. Furthermore, U.S. persons would be required to include contractual provisions in any covered data brokerage transaction with a foreign person prohibiting the recipient from entering into any subsequent covered data transaction involving the same data and a covered person.

Restricted and prohibited transactions

Most covered data transactions would effectively be subject to data security compliance requirements but would be permissible, assuming those requirements are met **prior** to entering into the transaction. This category, including vendor agreements, employment agreements, and investment agreements with covered persons, is referred to as restricted transactions. In effect, in order to be eligible to enter into covered data transactions with covered persons, a U.S. company will have to bring its data security program into compliance with federal rules before entering into the transaction.

The detailed security requirements are not yet known and will be the subject of a later rulemaking by the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA). However, the ANPRM generally

anticipates that they will be based on existing U.S. government standards related to basic cybersecurity posture, specified masking and privacy-preserving protocols, physical and logical access controls, and independent auditing of security controls.

The ANPRM **would presumptively prohibit two categories** of transactions with covered persons or countries of concern. Covered data transactions with covered persons or countries of concern involving **data brokerage** or involving the **bulk transfer of human genomic data (including investment transactions)** or biospecimens from which data can be derived would be prohibited absent a license.

Exemptions and licenses

The proposed regulatory framework is intended to narrowly target national security risks, and to this end the ANPRM proposes a variety of exemptions:

- Transactions conducted pursuant to official U.S. government business, such as by contractors and grantees;
- Intra-entity transactions between a U.S. person and its subsidiary or affiliate that is a covered person that are ordinarily incident to ancillary business operations (such as HR data);
- Certain financial and payment-related activities, such as those ordinarily incident to banking, capital markets, payment processing, financial insurance service, and related regulatory compliance activities; and
- Data transactions involving only personal communications and informational materials.

The last exemption bears additional scrutiny. The statutory authority for the Order is the IEEPA, the same statute underlying U.S. sanctions programs, ICTS reviews, and a number of other national security-related restrictions. IEEPA contains a statutory restriction, the so-called “Berman Amendment,” that denies the President authority to regulate, among other things, “any information or informational materials.” 50 U.S.C. § 1702(b)(3). While the exemption is to be spelled out in the final regulations and doubtless will purport to comply with the IEEPA restriction, it is not clear that IEEPA actually provides sufficient statutory authority to permit the President to regulate transfers of sensitive personal data. At least one recent court case challenging President Trump’s attempt to ban TikTok from the United States (also by executive order issued under the authority of IEEPA) held that IEEPA did not give the President authority to prohibit the export of users’ data to China. *TikTok v. Trump*, 507 F. Supp. 92 (D.D.C. 2020). It remains to be seen whether the proposed regulatory program would survive judicial scrutiny absent additional statutory authority.

The ANPRM also contemplates a licensing regime, modeled on that used by Treasury’s Office of Foreign Assets Control (OFAC), that would grant both general (blanket) and specific (case-by-case) licenses to engage in otherwise prohibited or restricted data transactions. The licensing regime will give DOJ additional flexibility in providing exceptions to the program’s restrictions.

Overlap with CFIUS

The investment provisions of the ANPRM are much broader than CFIUS’s jurisdiction. However, to avoid duplication, the ANPRM proposes that its provision would no longer apply to transactions in which CFIUS has exercised its jurisdiction to enter into or impose transaction-specific mitigation measures to resolve national security risks arising from the transaction that include some mitigation of data-security risks. The ANPRM would continue to apply to a transaction under CFIUS review unless and until such mitigation measures are imposed (meaning, for example, that an investment transaction subject to the ANPRM could not close during the pendency of CFIUS review unless the ANPRM’s requirements were already met.

Recordkeeping and enforcement

The ANPRM proposes to empower DOJ to seek civil penalties from those that “knowingly” violate regulations, or “should have known” of the circumstances giving rise to a violation. Unlike OFAC sanctions, this would not be a strict liability regime. In addition, the ANPRM proposes affirmative reporting obligations only in certain cases, such as annual certifications from those operating pursuant to a license, or from U.S. persons that engage in restricted data transactions and are more than 25% owned by a Covered Person. In addition, those engaging in restricted transactions may be required to fulfill limited “know your customer”-style affirmative due diligence and recordkeeping obligations. Whether or not these affirmative obligations are imposed, the ANPRM anticipates that (similar to other regulatory regimes) there will be an enforcement expectation that entities devise and implement a risk-based compliance program.

Next steps

Comments on the ANPRM are due April 19, 2024. The Order directs DOJ to publish a proposed rule by August 26, 2024; once that happens, there will be a second comment period on the proposed rule. Timing for finalization is unknown, as is the timing for CISA to publish the proposed security requirements for comment.

The Order also calls out several other areas for further study or in which agencies should consider further action, including:

- Directing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, generally known as Team Telecom, to address the risks of access to sensitive data through submarine cable systems and to issue policy guidance on the review of license applications for submarine cables;
- Directing various agencies to consider further steps to protect health and genomic data and to issue guidance to assist research entities in protecting such data; and
- Directing the intelligence community to recommend actions to address past transfers of sensitive personal data to countries of concern.

Practical takeaways

The ANPRM is far from being in final form, and the imposition of binding obligations is months away. The rules will not be retroactive, so no immediate action (other than submitting comments on the proposal) is required. CISA's promulgation of security requirements will be a critical step, and interested entities may wish to begin evaluating their data security programs as soon as possible in order to be eligible to continue to engage in covered data transactions with covered persons. They may also wish to evaluate the extent to which they currently engage in (or plan to engage in) covered data transactions to assess and mitigate their exposure to the regulations. All of these are matters that could require significant time to address.

In the medium to longer term, affected entities should anticipate implementation of a framework broadly similar to the ANPRM, which will have a wide-ranging impact on U.S. companies. For example, the workaday aggregation of otherwise innocuous data types, like those cited in the draft definition of "covered personal information," is effectively standard practice for many operating in e-commerce, marketing, business analytics and other data-intensive sectors. Hitherto unregulated companies may be caught off guard if their ordinary course analytics become a novel hook for regulatory scrutiny, and especially so when enforcement actions premised on security and controls failures that lead to inadvertent data loss are already commonplace. Affected stakeholders may wish to comment on definitional scope.

U.S. companies in data-intensive industries or that have or contemplate a significant international presence in a country of concern, such as China, should evaluate the extent to which current activities could fit within the ANPRM's exemptions, such as the exemption for intracompany data transfers incidental to ordinary business operations. They should also revisit their risk assessments and prepare for new compliance-related costs and obligations. This likely includes constructing an inventory of their current data collection activities and determining if they engage in any transactions involving bulk sensitive data or government-related data.

U.S. firms that sell data through data brokers or that transact in genomic data should determine if these transactions would be prohibited by the ANPRM and, if so, develop contingency plans to curtail those transactions or seek a license.

Finally, both foreign investors and U.S. companies should prepare for a significant impact on investment into the United States by covered persons, in particular Chinese investors. As a practical matter, direct investment of any size in data-intensive U.S. businesses by Chinese investors will become impossible unless the U.S. business has a compliant data security program in place prior to the investment or a license is obtained; investment in businesses holding U.S. genomic data may simply be prohibited. This could have a significant impact on transaction feasibility and timing. Foreign investors from countries of concern should begin to incorporate sensitive data considerations into their diligence processes, including steps to assess data inventory and security controls, and U.S. companies seeking investors may wish to position themselves in advance to be able to accept restricted investments.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Robert A. Cohen
+1 202 962 7047
robert.cohen@davispolk.com

David I. Feinstein
+1 212 450 3293
david.feinstein@davispolk.com

James W. Haldin
+1 212 450 4059
james.haldin@davispolk.com

Daniel S. Kahn
+1 202 962 7140
daniel.kahn@davispolk.com

Paul Marquardt
+1 202 962 7156
paul.marquardt@davispolk.com

Paul J. Nathanson
+1 202 962 7055
+1 212 450 3133
paul.nathanson@davispolk.com

Martin Rogers
+852 2533 3307
martin.rogers@davispolk.com

Will Schisa
+1 202 962 7129
will.schisa@davispolk.com

Paul S. Scrivano
+1 650 752 2008
+1 212 450 4304
paul.scrivano@davispolk.com

Daniel P. Stipano
+1 202 962 7012
dan.stipano@davispolk.com

1 89 Fed. Reg. 15421 (Feb. 28, 2024).

2 *Id.*

3 Department of Justice, *Justice Department to Implement Groundbreaking Executive Order Addressing National Security Risks and Data Security* (Feb. 28, 2024) ("DOJ Press Release"), *available at* https://www.justice.gov/opa/pr/justice-department-implement-groundbreaking-executive-order-addressing-national-security.

4 *See* National Intelligence Council, NICA 2020-027: Cyber Operations Enabling Expansive Digital Authoritarianism (Declassified Oct. 5, 2022), https://www.dni.gov/files/ODNI/documents/assessments/NICM-Declassified-Cyber-Operations-Enabling-Expansive-Digital-Authoritarianism-20200407—2022.pdf