

DOJ and CISA Propose New National Security Program to Regulate Foreign Access to Sensitive Data

October 24, 2024

On October 21, 2024, the U.S. Department of Justice (Department or DOJ) and the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) issued proposals – required by the President's February 2024 Executive Order 14117 – that together, if adopted, will establish a new regulatory framework aimed at *"Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern."* Specifically:

- DOJ released a Notice of Proposed Rulemaking (NPRM) – which follows the DOJ's March 2024 Advanced Notice of Proposed Rulemaking (ANPRM) in the same proceeding – that proposes a new national security program that would establish (1) certain countries of concern and classes of covered persons with whom transactions involving Government-related data or bulk U.S. sensitive personal data would be prohibited or restricted; (2) specified classes of prohibited and restricted transactions; (3) a process to issue, modify, or rescind licenses authorizing otherwise prohibited or restricted transactions; (4) a process to issue advisory opinions; and (5) recordkeeping and reporting on transactions to inform investigative, enforcement, and regulatory efforts of the Department. Under the DOJ's proposed new framework, the sensitive personal data that would trigger prohibitions and restrictions include biometric, genomic, financial, geolocation, and health data, along with certain personal identifiers, that exceed bulk thresholds. The NPRM is complex and detailed – totaling 422

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law
Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
lbrown@wiley.law

Sydney M. White
Special Counsel
202.719.3425
swhite@wiley.law

Practice Areas

National Security
Privacy, Cyber & Data Governance
Telecom, Media & Technology

pages.

- Concurrently, CISA released Proposed Security Requirements for Restricted Transactions under EO 14117.

Given the scale and breadth of the proposed new framework, the proposed new rules and requirements will likely impact a wide range of commercial transactions and relationships. Stakeholders have the opportunity to weigh in with written comments on both the DOJ's NPRM and CISA's Proposed Security Requirements. Comments on each proposal will be due 30 days after its publication in the Federal Register.

Below, we provide key context for the DOJ's and CISA's latest moves, as well as a summary of new proposals.

Proposals Are Next Steps in Administration's Efforts to Address National Security Risks of Sensitive Data Getting into the Hands of Countries of Concern

Both the DOJ's and CISA's proposals stem from ongoing concerns from the Biden Administration that access by "countries of concern" to Americans' sensitive data raises risks for national security, including cybersecurity risks.

This concern was the impetus behind the President's February 2024 Executive Order 14117 on *Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern*, which tasked the DOJ with issuing regulations restricting acquisitions or other transfers of U.S. Government-related data and bulk U.S. sensitive personal data to foreign countries or nationals that have been deemed U.S. adversaries and CISA with addressing "security requirements that might mitigate the risk of access by countries of concern to data from restricted transactions that will be available for public comment."

Shortly after the Executive Order (EO) was issued, the National Security Division of the DOJ issued an ANPRM seeking public comment on proposed rules implementing the EO. In response to the comments received on the ANPRM, the DOJ has now issued the current NPRM.

The NPRM Proposes Six Countries of Concern and Defines Classes of Covered Persons

As previewed in the ANPRM, the NPRM designates six countries as countries of concern for purposes of the proposed restrictions: China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela.

In addition to these countries, the NPRM identifies four categories of covered persons that face similar restrictions:

1. Foreign entities that are 50% or more owned by a country of concern, organized under the laws of a country of concern, or has its principal place of business in a country of concern;
2. Foreign entities that are 50% or more owned by a covered person;
3. Foreign employees or contractors of countries of concern or entities that are covered persons; and

4. Foreign individuals primarily resident in countries of concern.

To the extent an individual or entity does not fall into these categories, but the DOJ determines them to be, or to have been, controlled by or under the jurisdiction of a country of concern or a covered person, or who acts, has acted, or is likely to act on behalf of such entities, or who knowingly causes or is likely to cause a violation of this part, such persons or entities will be identified in a public list of additional restricted entities.

The NPRM Proposes to Regulate (1) Sensitive Personal Data, Broadly Defined to Include Covered Personal Identifiers, Precise Geolocation Data, Biometric Identifiers, Human Genomic Data, Personal Health Data, and Personal Financial Data; and (2) Government-Related Data

Sensitive Personal Data. The Department proposes to define “six categories of ‘sensitive personal data’ that could be exploited by a country of concern to harm U.S. national security if that data is linked or linkable to any identifiable U.S. individual or to a discrete and identifiable group of U.S. persons.” The six categories are:

1. Covered personal identifiers (e.g., names linked to device identifiers, social security numbers, driver’s license, or other government identification numbers);
2. Precise geolocation data (e.g., GPS coordinates);
3. Biometric identifiers (e.g., facial images, voice prints and patterns, and retina scans);
4. Human genomic data (e.g., DNA within each of the 24 distinct chromosomes in the cell nucleus, including results from genetic testing);
5. Personal health data (e.g., height, weight, vital signs, symptoms, test results, diagnosis, and psychological diagnostics); and
6. Personal financial data (e.g., information related to an individual’s credit, debit cards, bank accounts, and financial liabilities, including payment history).

The Department assessed the sensitivity of each category of sensitive personal data, and indicated that human genomic data, biometric identifiers, and precise geolocation information are the three most sensitive categories. Of note, precise geolocation data is defined under the proposed rule as “as data, whether real-time or historical, that identifies the physical location of an individual or a device with a precision of within 1,000 meters,” which is distinct from the definition of “precise geolocation information” under the *Protecting Americans’ Data from Foreign Adversaries Act of 2024 (PADFA)*, a similar but distinct new federal law that went into effect in June 2024.

Excluded Data. Also previewed in the ANPRM, the Department proposes to categorically exclude certain categories of data from the definition of the term “sensitive personal data,” such as public or nonpublic data that do not relate to an individual (e.g., trade secrets and proprietary information) and data that is already lawfully publicly available from government records or widely distributed media. Further, personal communications, data incident to travel, and certain informational (expressive) materials are exempt to the extent they are exempt from regulation under the International Emergency Economic Powers Act (see later discussion of exemptions).

Bulk Sensitive Personal Data Thresholds. The proposed rule's prohibitions and restrictions would generally apply only to covered data transactions involving sensitive personal data that exceeds certain bulk volume thresholds. The proposed rule would establish the following bulk thresholds:

- Human genomic data on over 100 U.S. persons;
- Biometric identifiers on over 1,000 U.S. persons;
- Precise geolocation data on over 1,000 U.S. devices;
- Personal health data on over 10,000 U.S. persons;
- Personal financial data on over 10,000 U.S. persons;
- Certain covered personal identifiers on over 100,000 U.S. persons; or
- Any combination of these data types that meets the lowest threshold for any category in the dataset.

These bulk thresholds would not apply to transactions involving certain Government-related data, which would be regulated regardless of the volume.

The NPRM Contemplates a Complex Framework of Prohibited, Restricted, and Exempted Transactions

Prohibited Transactions. Consistent with the ANPRM, the NPRM would limit or prohibit U.S. persons from engaging in certain classes of transactions that the DOJ deems to pose an unacceptable risk of giving countries of concern or covered persons access to U.S. Government-related data (including Government-Related Location Data List) or bulk sensitive personal data. The proposed rule would regulate transactions involving the six categories of data listed above that the Department defines as sensitive personal data that a country of concern or covered person could exploit to harm U.S. national security if that data is linked or linkable to any identifiable U.S. individual or to a discrete and identifiable group of U.S. persons.

Restricted Transactions. Beyond the prohibited transactions, the NPRM proposes to establish restrictions on a wider range of commercial transactions and relationships, to include vendor agreements, employment agreements, and non-passive investment agreements with countries of concern or covered persons.

These restricted transactions would only be permitted if they satisfy CISA's security requirements to mitigate risks from countries of concern or covered persons, which are also a forthcoming deliverable under EO 14117, as detailed further below.

Exempt Transactions. Based in part on stakeholder feedback, the NPRM includes additional data transaction exemptions beyond what the DOJ originally contemplated in the ANPRM. For example, in the NPRM, the DOJ proposes that data transactions will be exempt from the rule to the extent they are "ordinarily incident to and part of the provision of telecommunications services, including international calling, mobile voice, and data roaming." To provide guidance on the scope of this exemption, DOJ gives the example of a U.S. telecommunications service provider exchanging its U.S. subscribers' personal identifiers with a service provider in a country of concern for purposes of provisioning services to the U.S. service provider's U.S. subscribers in the country of concern. Under this example, even if the U.S. service provider were to exceed the

bulk threshold, the transfer for the provision of telecommunications services would be exempt.

Other proposed exemptions under the NPRM include exemptions for:

- Transactions incident to “financial services, such as banking, capital markets, or financial insurance services [and] transfer of personal financial data incidental to e-commerce”;
- Investment agreements subject to the Committee on Foreign Investments in the United States (CFIUS) mitigations;
- Drug, medical device, and biological product authorizations;
- Clinical trials regulated by the U.S. Food and Drug Administration;
- Corporate group transactions;
- Transactions required by federal law such as those on international civil aviation; and
- Official U.S. Government activities.

DOJ Contemplates Issuing Licenses and Advisory Opinions

The NPRM would authorize the DOJ, with concurrence from the Departments of State, Commerce, Homeland Security, and other relevant agencies, to issue general licenses allowing certain categories of otherwise restricted transactions to proceed under qualifying circumstances. The NPRM also would authorize the DOJ to issue specific licenses in response to applications from parties who disclose the details of their intended transactions. Both general and specific licenses may impose obligations on the recipient, such as disclosure, reporting, recordkeeping, due diligence, certification, and cybersecurity requirements. Approved licenses may be later modified or rescinded based on later obtained information. The NPRM also proposes a process for requesting reconsideration of denied license applications based on new or changed facts. Of note, the DOJ “anticipates that licenses will be issued only in rare circumstances.”

The proposal also establishes a process for DOJ, if requested, to issue advisory opinions addressing the interpretation and application of the regulations to specific – and real, not hypothetical – transactions.

The NPRM Proposes Recordkeeping and Reporting Requirements

As explained in the ANPRM, the NPRM does not contemplate any *general* due diligence recordkeeping, reporting, or compliance requirements for *all data transactions*. Instead, companies and individuals would be expected to develop and oversee their own compliance programs based on the unique aspects of their programs’ risk profiles.

The NPRM does, however, propose compliance requirements for U.S. persons engaging in *restricted transactions*, to include implementing a comprehensive internal compliance program, establishing written policies on data security and compliance, conducting annual audits, and maintaining an ongoing accuracy certification process for 10 years of certain data transfer records.

The NPRM also proposes the following reporting requirements for U.S. persons engaged in certain restricted transactions:

- Annual reports for U.S. persons engaged in restricted transactions involving cloud-computing services if the company is 25% or more owned by a country of concern or covered person;
- Reports for U.S. persons that have rejected an offer from another person to engage in a prohibited transaction involving data brokerage;
- Reports for U.S. persons engaged in a covered data transaction involving data brokerage with a foreign non-covered person if the U.S. person knows or suspects that the foreign non-covered person may violate resale restrictions and transfer the data to countries of concern or covered persons; and
- Reports for U.S. persons invoking the exemptions for certain data transactions covering regulatory approvals to market a drug, biological product, device, or a combination product in a country of concern.

Finally, the NPRM would authorize the DOJ to investigate potential violations of the new regulations, including holding hearings, deposing witnesses, and issuing subpoenas for witnesses and documents. Violators could face civil and criminal penalties, including fines and imprisonment.

CISA's Proposed Security Requirements Would Apply to Restricted Transactions Under the New Regulatory Framework.

As described above, CISA concurrently released its *Proposed Security Requirements for Restricted Transactions* on October 21, 2024, and those proposed security requirements will be open for public comment once published in the Federal Register. CISA's proposal – which it intends to be based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework, NIST Privacy Framework, and the CISA Cross-Sector Cybersecurity Performance Goals – would establish organizational-level, system-level, and data-level requirements for restricted transactions under the DOJ's proposed new framework. Proposed organizational level requirements include identifying assets in the covered system, designating governance structures, remediating known exploited vulnerabilities, documenting vendor agreements, implementing a process for approval of new equipment installation, and developing an incident response plan, among other things. Proposed system-level requirements include logical and physical access controls, enforcing multifactor authentication, collecting logs on covered systems, and securely storing logs. Proposed data-level requirements include data minimization, encryption, and privacy-enhancing technologies such as homomorphic encryption.

Wiley's Telecom, Media & Technology and Privacy, Cyber & Data Governance teams, along with the International Trade and National Security practices, have focused on privacy, security, digital trade, data localization, and related issues for decades. This includes advising companies in CFIUS reviews, negotiating data transfer agreements, and supporting compliance with various U.S. and international legal obligations related to the movement and use of data. Whether from a compliance or a policy perspective, our team can

address any questions about this EO or the work it has directed.