JENNER & BLOCK

DOJ and CISA Issue Proposals Addressing National Security Risks Posed to US Sensitive Data

Client Alerts

November 6, 2024
By: Madeleine Findley, Shoba Pillay, Emma O'Connor

On October 21, 2024, the US Department of Justice (DOJ) and the US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) released for comment proposals to implement President Biden's February 2024 Executive Order 14117 (the EO), "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern."[1] The proposed rules are framed as national security, rather than data privacy, regulations and will regulate transactions with certain "countries of concern" that involve bulk US sensitive personal data or US government-related data, which can be used for malicious purposes, including analysis and manipulation of such data to engage in espionage, influence, kinetic, and cyber operations against the United States. If adopted, the rule would establish the DOJ as a significant regulator of data flows and impose robust new compliance obligations on businesses that collect, process, and disclose data—including even small amounts of certain types of data—from US persons and have relationships with entities, including vendors, in countries such as China and Russia.

The DOJ's Notice of Proposed Rulemaking

The DOJ released a Notice of Proposed Rulemaking (NPRM),[2] which will implement the EO by establishing categorical rules for certain data transactions that pose a high risk of giving "countries of concern" or "covered persons" access to government-related data or bulk US sensitive personal data. The NPRM was published in the Federal Register[3] on October 29, 2024, and comments on the proposed rule may be submitted until November 29, 2024.

The proposed rule is largely consistent with the proposals in the DOJ's March 2024 Advanced Notice of Proposed Rulemaking[4] under the EO. It provides additional information regarding the thresholds for "bulk" sensitive personal data, security requirements, compliance obligations, and exempted transactions. Notably, the proposed rule will apply to any transaction, including investments, employment agreements, and vendor relationships, in which a US business gives

access to entities from "countries of concern" to "sensitive personal data and government-related data":

- Human genomic and human 'omic data (*i.e.*, nucleic acid sequences that constitute the whole or part of a person's genetic sequence) of 100 US persons;
- Biometric identifiers, including facial images, voice prints, and keyboard usage patterns, of more than 1,000 US persons;
- Precise geolocation data of more than 1,000 US persons;
- Personal financial data, including information about an individual's purchases and payment history, of more than 10,000 US persons;
- Personal health data of more than 10,000 US persons; and
- Covered personal identifiers, including full or truncated social security numbers, advertising data, and contact data, of more than 100,000 US persons.

The proposed rule will also prohibit certain transactions entirely, including transactions involving (1) data brokerage with a covered person or country of concern; (2) access by a covered person or country of concern to bulk US human genomic data or to biospecimens from which such data could be derived; or (3) data brokerage with any foreign person (other than a prohibited covered person) unless the US business or person contractually requires the recipient to retrain from engaging in an onward data transfer to countries of concern or covered persons.

Consistent with the EO, the "countries of concern" are China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela. The NPRM also provides that an entity is a "covered person" if it is a foreign person that: (1) is 50 percent or more owned, directly or indirectly, by a country of concern (or another covered person); (2) is organized or chartered under the laws of a country of concern; or (3) has its principal place of business in a country of concern. Any foreign individual who is an employee or a contractor of such an entity or of the country of concern or who is primarily a resident in the territorial jurisdiction of a country of concern is also a covered person. The DOJ retains the authority to supplement these categories with a public list of designated entities and individuals.

For businesses that collect or process personal data of US persons, the NPRM has far-reaching implications. For example, businesses that offer smartphone apps capable of collecting geolocation data, including through the use of a third party SDK, or that collect and process biometric data, such as facial recognition or gait measurements, will need to review their vendor relationships, partnerships, and employment agreements as well as their compliance programs for potential new compliance requirements or increased risk under the proposed rule.

Additionally, the proposed rule identifies processes for the DOJ to issue, modify, or rescind licenses authorizing otherwise prohibited or restricted transactions, and to issue advisory opinions addressing the interpretation and application of the regulations to specific transactions. It will empower the Attorney General to designate as "covered persons" any foreign third party that violates the rule, similar to the process for designation on sanctions lists maintained by the Office on Foreign Assets Control (OFAC). The proposed rule also addresses recordkeeping, reporting, and other due-diligence obligations for covered transactions. The proposed rule would require US persons engaging in restricted transactions to:

- Comply with the proposed CISA Security Requirements (discussed below);
- Implement and maintain a comprehensive internal data compliance program;
- Establish written policies on data security and compliance;
- Conduct annual third party audits; and
- Maintain records of each restricted transaction for 10 years after the date of the transaction.

The proposed rule does not include generalized data localization requirements to store Americans' bulk sensitive personal data or government-related data. The proposed rule also does not broadly prohibit US persons from engaging in commercial transactions, including exchanging financial and other data as part of the sale of commercial goods and services, with countries of concern or covered persons. And the proposed rule exempts several classes of data transactions from the scope of its prohibitions and restrictions, including certain personal communications, financial services, corporate group transactions, transactions authorized by federal law and international agreements, investment agreements subject to a Committee on Foreign Investment in the United States (CFIUS) action, transactions ordinarily incident to telecommunication services, biological product and medical device authorizations, clinical investigations, and others.

Notably, the proposed rule will 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.[5]

The proposed rule addresses public comments that the DOJ received on the Advance Notice of Proposed Rulemaking. In response to comments, the DOJ underscored that the proposed rule is a national security rule while generally declining to incorporate aspects of international or state privacy laws, explaining that privacy protections and national security measures share "some overlap," but "generally focus on different challenges associated with sensitive personal data."[6]

The proposed rule has a 30 day comment period. The public may submit written comments at www.regulations.gov.

CISA's Proposed Security Requirements for Restricted Transactions

Concurrent with the DOJ's proposed rule, and as required by the EO, CISA has published proposed security requirements.[7] These proposed security requirements obligate US persons engaging in a restricted transaction to comply with organizational and system-level standards, such as ensuring that basic cybersecurity policies and controls are in place, and data-level standards, such as implementing data minimization and masking techniques.

CISA's proposed requirements apply to the "restricted transactions" addressed by the DOJ's proposed rule, and "covered data" is also defined by CISA to mean bulk US sensitive data or government-related data. A "covered system" means any information system used to, among other things, obtain, read, copy, edit, process, disseminate, or dispose of covered data as part of a restricted transaction, regardless of whether the data is encrypted, anonymized, pseudonymized, or de-identified.

CISA's proposed organizational and system-level requirements would require "basic organization cybersecurity policies [and] practices,"[8] including:

- Maintaining a regularly updated inventory of covered system assets, with each system's respective internet protocol (IP) address (or, for hardware, MAC address);
- Ensuring inventory is updated on a recurring basis, and no less than monthly for Information Technology assets;
- Designating an individual responsible for cybersecurity and for governance, risk, and compliance functions *(e.g.*, a Chief Information Security Officer);
- Remediating known exploited vulnerabilities within 14 calendar days, and remediating other vulnerabilities within 15 calendar days if they are deemed to be of "critical severity," and within 30 calendar days if they are deemed to be of "high severity";
- Documenting and maintaining all vendor / supplier agreements for covered systems;
- Developing and maintaining an accurate network topology of the covered system;
- Adopting and implementing an administrative policy that includes a manual or automated process that requires approval before new hardware, firmware, or software is installed in a covered system; and
- Developing and maintaining incident response plan(s), to be reviewed annually and updated as appropriate.

Additionally, at an organizational and system level, CISA will require the implementation of logical and physical access controls to prevent covered persons or countries of concern from gaining access to covered data, in any form. Specifically, US persons engaging in restricted transactions would be required to:

- Enforce multifactor authentication (MFA) on all covered systems, or, in instances where MFA is not feasible, require passwords to have sufficient strength (*e.g.,* contain 16 or more characters);
- Immediately revoke, upon termination or change in roles for any individual with authorized access to covered system(s), any credentials assigned to that individual;
- Collect logs for covered systems pertaining to access and security focused events (*e.g.*, the detection of unsuccessful login events);
- Maintain organizational policies and processes to ensure that unauthorized media and hardware are not connected to covered assets, such as by limiting the use of USB devices;
- Implement configurations to deny by default all connections to covered systems and their networks, unless connections are explicitly allowed for specific system functionality; and
- Issue and manage identities and credentials for authorized users, services, and hardware, with sufficient attributes to prevent unauthorized access.

Under CISA's proposed requirements, US persons engaging in restricted transactions would also have to conduct and document a data risk assessment, to be reviewed annually and updated as appropriate.

At a data level, CISA's proposal would require, for any restricted transaction, the implementation of a combination of the following risk mitigation measures:

- Data minimization and data masking strategies, including the implementation and maintenance of an annually reviewed data retention and deletion policy, and the processing of data in such a way as to either render it no longer covered data or minimize the linkability to US persons before it is subject to access by a covered person or country of concern;
- Encryption techniques to protect covered data during the course of restricted transactions, including comprehensive encryption, Transport Layer Security (TLS), and the secure management of cryptographic keys;
- The application of privacy enhancing technologies, such as privacy preserving computation (*e.g.*, homomorphic encryption), or differential privacy techniques to process covered data; and
- The configuration of identity and access management techniques to deny authorized access to covered data by covered persons and countries of concern within all covered systems.

CISA is concurrently making these proposed security requirements available for public comment at www.regulations.gov.

Key Takeaways

The complex, detailed new framework that will be created by the DOJ's proposed rule and CISA's proposed requirements will affect a broad range of commercial transactions and industries, including transactions involving large institutional investors. Affected industries include but are not limited to: healthcare providers; research institutions; information technology service providers; technology companies that collect large amounts of users' personal information, including big data analytics and artificial intelligence companies; social media companies; large online marketplaces; insurance providers; biotechnology companies; and ancestry and DNA testing companies; along with the employees, vendors, and other third parties with whom companies in such industries do business.

The DOJ included over two hundred pages of supplemental analysis in the NPRM, including numerous examples illustrating the rationale and scope of the proposed regulation. These materials emphasize the intentionally broad sweep of the proposed rule beyond even the entities directly referenced. As a result, all businesses that collect and process the covered data categories should monitor how this rulemaking will impact their data practices, including relationships with vendors in "countries of concern," and take steps to be prepared for additional and burdensome compliance and security requirements.

Potentially affected businesses should consider:

- Filing or joining comments to better inform the proposals;
- Reviewing whether their operations involve cross-border data transactions with any "countries of concern" or "covered persons" that include bulk amounts of US sensitive personal data or any US government-related data; and
- Reviewing their vendor, employment, and investment agreements.

We will continue to monitor developments and provide updates as the proposals are reviewed and adopted, and as US federal agencies begin to implement and enforce this new data transaction regulatory regime.

Footnotes

[1] Executive Order 14117, *Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern*, 89 FR 15421 at Sec. 1 (Feb. 28, 2024), https://www.whitehouse.gov/briefing-room/presidential-

actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/.

[2] Department of Justice, Office of the Attorney General, *Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons*, 28 CFR Part 202, RIN 1124-AA01 (Oct. 21, 2024), https://www.justice.gov/d9/2024-10/nsd_104_-_data_security_-_1124-aa01_-_notice_of_proposed_rulemaking_0.pdf.

[3] "Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons," Federal Register (Oct. 29, 2024), https://www.federalregister.gov/documents/2024/10/29/2024-24582/provisions-pertaining-to-preventing-access-to-us-sensitive-personal-data-and-government-related-data.

[4] "National Security Division; Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern." 28 CFR Part 202 (Mar. 5, 2024), https://www.govinfo.gov/content/pkg/FR-2024-03-05/pdf/2024-04594.pdf.

[5] 28 CFR Part 202, RIN 1124-AA01, at 410, 416.

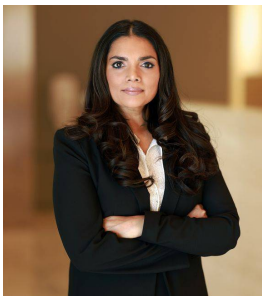
[6] *Id.* at 21.

[7] Cybersecurity & Infrastructure Security Agency, *Propose Security Requirements for Restricted Transactions Pursuant to Executive Order 14117* (Oct. 21, 2024), https://www.cisa.gov/sites/default/files/2024-10/Proposed-Security-Requirements-EO-14117-21Oct24508.pdf.

[8] *Id.* at 2.

Related Attorneys

Madeleine Findley
Partner
mfindley@jenner.com
+1 202 639 6095



Shoba Pillay
Partner
spillay@jenner.com
+1 312 923 2605

Emma O'Connor
Associate
eoconnor@jenner.com
+1 202 639 3863

Related Capabilities

Data Privacy and Cybersecurity

Stay Informed →