Privacy + Security Forum

May 7, 2025

Locking It Down

A Deep Dive on the DOJ's Data Security Program Rule

Jeanine McGuinness | Partner, International Trade & Investment
Matthew Coleman | Partner, Cyber, Privacy & Data Innovation

orrick

DOJ's Data Security Program Rule

Agenda

- Background
- Key Concepts
  - Countries of Concern
  - Covered Person
  - Covered Data
  - Prohibited Transactions
  - Restricted Transactions
  - Exempt Transactions
- Implementation and Enforcement Policy
- Operationalizing The Rule
- International Trade Context

Background

How Did We Get Here?

- **May 15, 2019:** Executive Order 13873 – "*Securing the Information and Communications Technology and Services Supply Chain*"
- **February 28, 2024:** Executive Order 14117 – "*Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern*"
- **March 5, 2024**: DOJ issued Advance Notice of Proposed Rulemaking soliciting public comment
- **October 29, 2024:** DOJ issued Notice of Proposed Rulemaking – 89 FR 86116; CISA published Security Requirements for Restricted Transactions Under Executive Order 14117 – 89 FR 85976
- **January 8, 2025:** Final Rule published in the Federal Register – 28 CFR Part 202; Final CISA Rule published in the Federal Register – 90 FR 1528
- **April 8, 2025:** Effective Date of the Rule
- **April 11, 2025:** DOJ released an Implementation and Enforcement Policy, a Compliance Guide, and a list of over 100 Frequently Asked Questions (FAQs)
- **July 8, 2025:** End of 90-day grace period
- **October 6, 2025:** Companies engaging in restricted transactions have until October 6, 2025, to develop the required compliance programs

Key Concepts

Data Brokerage

- The rule defines data brokerage as:
  - the sale of data, licensing of access to data, or similar commercial transactions, excluding an employment agreement, investment agreement, or a vendor agreement, 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.

EXAMPLE

Data Brokerage

- We Like Locks, Inc. (a U.S. company) owns and operates a mobile app for U.S. users with available advertising space. As part of selling the advertising space, WLL provides IP addresses and advertising IDs of more than 100,000 U.S. users' devices to an advertising exchange based in a country of concern in a twelve-month period. Is this data brokerage?
  - **Answer:** Yes. The U.S. company's provision of this data as part of the sale of advertising space is a covered data transaction involving data brokerage and is a prohibited transaction because IP addresses and advertising IDs are listed identifiers that satisfy the definition of bulk covered personal identifiers in this transaction.

Countries of Concern

- Country of Concern: any foreign government determined by the Attorney General with the concurrence of the Secretary of State and the Secretary of Commerce to:
  - Have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the U.S. or security and safety of U.S. persons; and
  - Pose a significant risk of exploiting government-related data or bulk U.S. sensitive personal data to the detriment of the national security of the U.S. or security and safety of U.S. persons.
- The rule establishes **China (including the Special Administrative Regions of Hong Kong and Macau), Cuba, Iran, North Korea, Russia and Venezuela** as Countries of Concern.

Covered Person

Covered Persons include:

Entities:

- That are organized in a Country of Concern;
- That have a principal place of business in a Country of Concern;
- That are designated by DOJ as a Covered Person; or
- That are 50% or more owned, directly or indirectly, individually or in the aggregate, by one or more Countries of Concern or Covered Persons.

Individuals:

- That are employees or contractors of a Country of Concern or a Covered Person;
- That are residents of China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia or Venezuela; or
- That are designated by DOJ as a Covered Person.

DOJ will maintain a public list of designated Covered Persons. The rule authorizes DOJ to designate persons upon the basis of ownership or control by, or acting for on behalf of, a Covered Person or Country of Concern. Being subject to the jurisdiction of a Country of Concern, or knowingly causing a violation of the rule, are also bases for designation.

COVERED DATA

Bulk Sensitive Personal Data

The term bulk U.S. sensitive personal data means a collection or set of sensitive personal data relating to any U.S. persons, in any format, regardless of whether the data is anonymized, pseudonymized, de-identified or encrypted, that exceeds the specified thresholds.

COVERED DATA

Bulk Sensitive Personal Data Thresholds

- **Covered Personal Identifiers:** 100,000 U.S. persons
- **Precise Geolocation Data:** 1,000 U.S. devices
- **Biometric Identifiers:** 1,000 U.S. persons
- **Human ‘omic Data:** 1,000 U.S. persons, or in the case of human genomic data, more than 100 U.S. persons
- **Personal Health Data:** 10,000 U.S. persons
- **Personal Financial Data:** 10,000 U.S. persons

U.S. Government-Related Data

- The rule defines U.S. government-related data as:
  - Precise geolocation data for any location within an enumerated list of specific geofenced areas associated with military, government and other sensitive locations.
  - 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 those in the military and intelligence community.

Prohibited Transactions

- The rule prohibits three categories of “highly sensitive” covered data transactions:
  - Data brokerage transactions involving Countries of Concern or Covered Persons.
  - Data brokerage transactions with non-covered foreign persons unless the U.S. person contractually requires the foreign person to refrain from engaging in a covered data transaction involving the same data with a Country of Concern or Covered Person. The rule also requires U.S. persons to report violations by foreign parties.
  - Transactions that provide a Country of Concern or Covered Person access to bulk human ‘omic data or human biospecimens from which human ‘omic data can be derived.
- NSD may also issue general or specific licenses to authorize certain transactions that would otherwise be prohibited.

Restricted Transactions

- The rule restricts the following three categories of covered data transactions by prohibiting them, **unless** they comply with security requirements issued by CISA. CISA recently finalized these requirements in a separate rulemaking.
  - Vendor agreements, including technology services and cloud service agreements such as Software-as-a-Service (SaaS).
  - Employment agreements, including employment on a board or committee, executive-level agreement and employment services at an operational level.
  - Investment agreements, including investments in U.S. real estate or legal entities.
- Triggers an audit requirement.

Exempt Transactions

- The rule exempts certain data transactions, including, among others, those:
  - Involving personal communications.
  - Ordinarily incident to travel to or from any country.
  - For the conduct of the official business of the U.S. government (including federally funded research).
  - Ordinarily incident to and part of the provision of **financial services**.
  - Between a U.S. person and its subsidiaries and affiliates located in (or otherwise subject to the ownership, direction, jurisdiction, or control of) a Country of Concern, to the extent that the transactions are incidental to administrative or ancillary business operations.
  - Ordinarily incident to and part of the provision of telecommunications services.

Exempt Transactions: Financial Services

- Banking, capital markets, or financial-insurance services
- A financial activity authorized for national banks (Office of the Comptroller of the Currency)
- An activity that is “financial in nature or incidental to such financial activity” or “complementary to a financial activity” (Federal Reserve)
- The transfer of personal financial data or covered personal identifiers ***incidental to 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)
- The provision or processing of payments or funds transfers (such as person-to-person, business-to-person, and government-to-person funds transfers) involving the transfer of personal financial data or covered personal identifiers, or the provision of services ancillary to processing payments and funds transfers
- The provision of investment-management services that manage or provide advice on investment portfolios or individual assets for compensation or provide services ancillary to investment-management services (such as broker-dealers or futures commission merchants)

Additional Requirements

The rule prohibits attempts to violate the prohibitions by evading their application (§ 202.304) or knowingly directing such a prohibited or restricted transaction (§ 202.305).

It also requires any U.S. person engaging in any transaction subject to the provisions of the Rule to keep a full and accurate record of each transaction engaged in to be available for examination for 10 years after the date of the transaction. (§ 202.1101).

A report must be filed by any U.S. person that receives and affirmatively rejects (including by way of automated tools) an offer from another person to engage in a prohibited transaction involving data brokerage. The report is due within 14 days of rejecting the transaction. (§ 202.1104).

Implementation and Enforcement Policy

Implementation & Enforcement Policy

- DSP Implementation and Enforcement Policy: An overview of enforcement mechanics, which indicates that DOJ will not prioritize civil enforcement actions for 90 additional days, provided good-faith efforts to comply are taken in the interim.
- The Implementation and Enforcement Policy outlines examples of how companies can demonstrate good-faith effort, including:
  - Internal reviews of potential data brokerage transactions
  - Negotiating onward transfer provisions in vendor and agreements
  - Relocating employees or vendor support services
  - Implementing CISA's security requirements

Penalties

- The International Emergency Economic Powers Act ("IEEPA") and the DSP authorize the National Security Division of the DOJ to bring civil enforcement actions and criminal prosecutions for knowing or, with respect to criminal prosecutions, willful violations of the DSP's requirements.
- Unlawful acts under IEEPA are subject to civil penalties of up to the greater of $368,136 (subject to adjustment for inflation) or twice the value of each violative transaction. Willful violations of IEEPA are punishable by imprisonment of up to 20 years and a $1,000,000 fine.

Operationalizing the Rule

Data Mapping

- Diligence on existing data flows to identify data brokerage transactions involving:
  - Bulk Sensitive Personal Data or U.S. Government-Related Data; or
  - Transactions involving Countries of Concern or Covered Persons
- Assess the purpose and context of the transfer to determine exemptions
- Leverage existing processes

Diligence (KYC/KYV)

- Diligence on customers, vendors, employees and investors
- Leverage existing processes
- Knowledge requirement
  - Covered Persons List
  - Review of influence or control not required
  - Not applicable to exempt transactions
- Know Your Data

CISA Security Requirements for Restricted Transactions

- Sets out security and data standards for restricted transactions.
- Organizational- and System-Level Requirements
- Data-Level Requirements
  - Data minimization and data masking strategies
  - Encryption in transit and at rest
  - Privacy enhancing technologies
  - Identity and access management

Contracting

- With foreign persons:
  - Onward transfer restrictions
  - Reporting requirements
- Generally:
  - Onward transfer restrictions

Retention

- U.S. persons engaged in restricted transactions must retain audit reports for a period of at least 10 years.
- U.S. persons engaging in any transaction subject to the DSP must keep a full and accurate record of each such transaction engaged in, and such record shall be available for examination for at least 10 years.
- Not applicable to exempt transactions, except to the extent required as a condition of a specific exemption.

EXAMPLE

Covered Person Acting on Behalf of Non-Covered Person

- Five out of nine board members of We Like Locks, Inc. are Covered Persons, but these persons own only 25% of the company, collectively. WLL is not otherwise established or operating in a Country of Concern, and nor does it qualify as a Covered Person. It has not been designated as a Covered Person by NSD. Is WLL a Covered Person?
  - **Answer**: No. Control is not a factor. Ownership is.
- One of the Covered Person board members is also the CEO of We Like Locks. Can a U.S. Person sign an agreement with the CEO to engage in a covered data transactions?
  - **Answer:** No. The covered person's signature, even if on behalf of a non-covered person like We Like Locks, constitutes a covered data transaction and would fall within the scope of the DSP's prohibitions and restrictions

EXAMPLE

Financial Services Exception

- Can a U.S. bank, as ordinarily incident to and part of facilitating payments to U.S. persons in China, store and process the customers' bulk financial data using a data center operated by a third-party service provider in China?
  - **Answer:** Yes. The use of this service provider is a vendor agreement; it involves access by a covered person to personal financial data, but it is an exempt transaction that is ordinarily incident to and part of facilitating international payment.
- What if underlying payments are between U.S. persons in the United States and do not involve China?
  - **Answer:** No. The use of the service provider in China, although it is a vendor agreement, is not exempt because it involves access by a covered person to bulk personal financial data and is **not ordinarily incident to facilitating this type of financial transaction**.

International Trade Context

Broader National Security Context

- The Data Security Program is one more tool the U.S. government has implemented to prevent China, Russia, Iran, and other foreign adversaries from engaging in activities it believes undermine U.S. national security and in particular exploit U.S. government-related data and Americans' sensitive personal data.
- It builds on other U.S. government programs aimed at containing China and other foreign adversaries.
  - We will discuss a few examples of these programs.

Committee on Foreign Investment in the United States (CFIUS)

- The statute authorizing CFIUS was last amended in 2018 during the first Trump administration.
  - The Foreign Investment Risk Review Modernization Act expanded CFIUS's jurisdiction to cover certain non-controlling investments by foreign persons in U.S. businesses that, among other things, maintain or collect certain types of sensitive personal data of U.S. citizens.
- CFIUS can impose mitigation conditions on parties to grant clearance of transactions.
  - For example, CFIUS may require transaction parties to adopt controls to protect sensitive personal data, such as by mandating that certain facilities, equipment, and operations are located only in the United States.

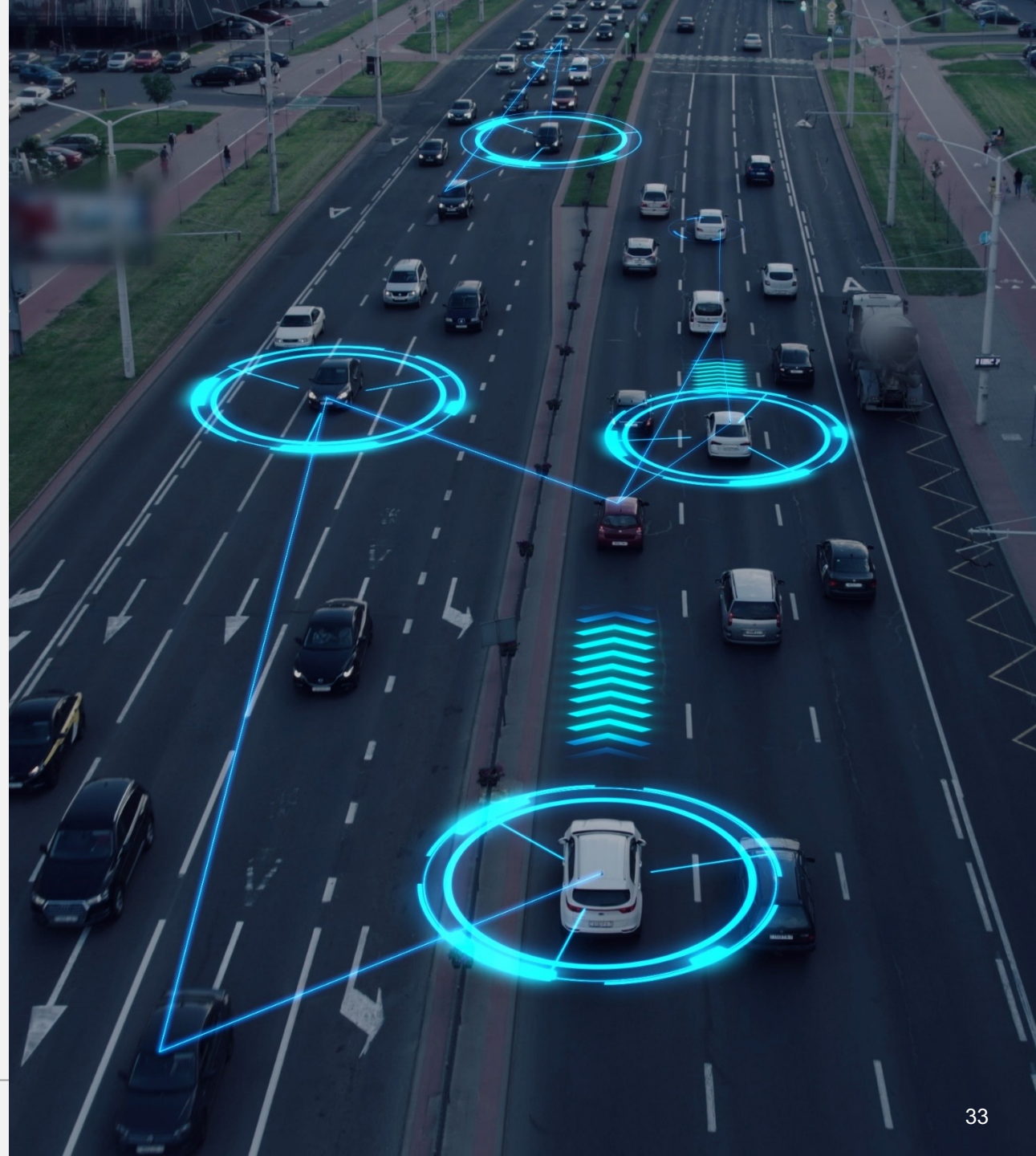
Information and Communications Technology and Communications Services (ICTS) Program

- In December 2024, the Commerce Department issued a final rule to formalize its information and communications technology and services (ICTS) program under Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain, issued by President Trump during his first term.
  - The rule authorizes the Secretary of Commerce to review, prohibit, or impose mitigation measures on certain transactions that involve ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary, including China and Russia, and that pose an undue or unacceptable risk to U.S. national security.
  - ICTS includes, among other things, software, hardware, or any other product or service integral to data hosting, computing or storage that **uses, processes or retains sensitive personal data**.

SPECIFIC ICTS RULE

Automated Driving Systems and Vehicle Connectivity Systems

- In January 2025, the Commerce Department issued a specific ICTS rule that, starting in several years, will prohibit the import or sale in the United States of certain software and hardware “designed, developed, manufactured, or supplied by” persons owned or controlled by or subject to the jurisdiction or direction of China or Russia that directly enable connected vehicle Automated Driving Systems (ADS) or Vehicle Connectivity Systems (VCS).
- The Commerce Department indicated that the rule is designed “to safeguard U.S. national security and protect Americans’ privacy by keeping foreign adversaries from manipulating these technologies to access sensitive or personal information.”



Questions?