User's Guide to DOJ & CISA Rules Implementing Executive Order 14117

Perkins Coie

Executive Order (EO) 14117 is a national security rule intended to mitigate national security risks posed by threat countries' access to sensitive personal data and government-related data. The EO directed the U.S. Department of Justice (DOJ) to issue implementing regulations and directed the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) to develop related security measures for classes of transactions.

DOJ and CISA each issued their final rules, which were published in the Federal Register on January 8, 2025 (*see* DOJ and CISA notices). The EO was not rescinded by President Trump's January 20, 2025, EO rescinding EOs issued by President Biden. Because the rules were published before the Presidential transition, President Trump's January 20, 2025 EO freezing pending regulations did not withdraw the DOJ or CISA rules, but they are subject to postponement for 60 days if DOJ or CISA identify a need to review a question of fact, law, or policy that the rules implicate.

This summary gives an overview of the substantive rule DOJ announced. Separate pieces will describe DOJ's anticipated compliance and enforcement regimes and the CISA security standards the rule cross-references.

The effective date of the rule is April 8, 2025. If the Trump administration postpones implementation to conduct a review, the effective date will be extended to June 9, 2025.

Contents

I. Overview

The rule is *not* a privacy rule. It is a national security rule. As a result, although privacy regimes and the rule cover much of the same territory, the rule is drafted with a different approach that may be unfamiliar to data privacy professionals. For example, the rule does not exempt encrypted, aggregated, or anonymized data from its scope. It does not distinguish among different categories of participants in a data transaction or between controllers and processors of data. Terms such as "data brokerage" refer to a type of data transfer, not to a specific category of business. And user consent is not relevant to the application of the rule.

The rule regulates types of transactions, not types of businesses. For example, the rule applies to personal health data regardless of whether the transacting party is covered under Health Insurance Portability and Accountability Act (HIPAA).

The rule regulates U.S. persons engaging in transactions that would provide "Countries of Concern" (CoCs), whether directly or through persons subject to their control or jurisdiction ("Covered Persons," or CPs), with data or access to data that constitutes bulk U.S. sensitive personal data (BUSPD) or U.S. government-related data. TheEO addresses four categories of such "Covered Data Transactions": (1) data brokerage transactions; (2) vendor agreements; (3) employment agreements; and (4) investment agreements. It prohibits data brokerage transactions involving BUSPD or government-related data with CoCs and CPs and restricts vendor, employment, and investment agreements that provide CoCs or CPs access to such data.

In almost all instances, the rule only covers data transactions that involve a U.S. person giving data or access to data to a CoC or CP. It does not cover transactions between two U.S. persons. If a U.S. person engages in a covered data brokerage transaction with a foreign person (FP) that is not a CP or CoC, however, the U.S. person must contractually obligate the FP not to engage in further data brokerage of the same data with a CoC or CP.

The rule applies a "knowingly" standard, meaning that a U.S. person only implicates the rule if they know, or reasonably should know, that they are engaging in transactions subject to the rule.

The rule exempts certain transactions, such as the transfer of information ordinarily incident to communications or financial transactions.

DOJ expressly rejected exempting data transactions conducted under contractual secrecy or privacy obligations. If a U.S. person's contract with a CP requires the CP to keep information confidential, that has no impact on the rule's application.

II. Role and Scope of "Knowingly" Standard – Third-Party Provider Considerations

The rule prohibits and restricts U.S. persons from "knowingly" engaging in covered data transactions. "Knowingly" means, with respect to conduct, a circumstance, or a result, that a U.S. person "had actual knowledge of, or reasonably should have known about" the conduct, circumstance, or result. DOJ expressly stated that this standard neither imposes strict liability nor is intended to require a U.S. person engaging in a data transaction with an FP to conduct due diligence on the counterparty's employment practices. But willful blindness will not shield a U.S. person from liability.

DOJ repeatedly rejected an exemption for third-party providers such as cloud platforms and subsea cable operators. Instead, DOJ emphasized that under the "knowingly" standard, a third-party provider is not required to take affirmative steps to discover whether its customers are engaging in covered data transactions and is only responsible for transactions of which it has actual knowledge or reasonably should know.

Examples distinguish between a U.S. operator of a fiber optic cable that has no reason to know the content of traffic transmitted on the cable, and therefore would not be liable for prohibited or restricted transactions

conducted on the cable, and a U.S. cloud service provider that specializes in processing sensitive data and therefore reasonably should know that a customer's transactions may involve sensitive data.

Moreover, a platform provider is not "knowing" of the kind or volume of data a customer processes on the platform even if the provider is "generally aware" of the customer's business and can access the customer's data *only* for troubleshooting and technical support.

28 C.F.R. § 202.230

III. Countries of Concern and Covered Persons

CoCs are designated by the attorney general. Currently, CoCs consist of the:

- People's Republic of China (PRC), including the Special Administrative Region of Hong Kong and the Special Administrative Region of Macau;
- Russian Federation;
- Islamic Republic of Iran;
- Democratic People's Republic of Korea (DPRK or "North Korea");
- Republic of Cuba; and
- Bolivarian Republic of Venezuela.

A "United States Person" or "U.S. Person" is any:

- U.S. citizen, national, lawful permanent resident, asylee, or refugee;
- Entity organized *solely* under the laws of the United States or any jurisdiction within the United States (including foreign branches); and
- Any person *in* the United States.

Any person that is not a U.S. person is an FP. A CP is an FP that:

- Is 50% or more owned by CoCs;
- Is organized or chartered under the laws of a CoC;
- Has its primary place of business in a CoC;
- Is 50% or more owned by CPs;
- Is a contractor of a CoC or CP; or
- Is primarily resident in a CoC.

The Attorney General can also designate any person, whether U.S. or foreign, as a CP.

28 C.F.R. §§ 202.211, 202.221, 202.255.

IV. Data Subject to the Rule

The rule covers "sensitive personal data" in bulk and "government-related data" in any amount.

A. Government-Related Data Defined

1. Precise geolocation data for locations in any area enumerated in a government-published list; or

2. Sensitive personal data marketed as linked or linkable to current or former U.S. Government employees, high-level officials, or contractors.

28 C.F.R. § 202.222

B. Sensitive Personal Data Defined

1. Covered personal identifiers (combinations of listed identifiers, described below);
2. Precise geolocation data, which does *not* include IP addresses;
3. Biometric identifiers (*e.g.*, facial images, voice prints and patterns, and retina scans), including biometric identifiers derived from public photos scraped from social media platforms (e.g., for training facial-recognition software);
4. Human genomic data (*e.g.,* DNA, including results from genetic testing), including the results of individual genetic testing and related sequencing data;
5. Personal health data (*e.g.*, height, weight, vital signs, symptoms, test results, diagnosis, psychological diagnostics, treatment history, exercise logs, immunization data, prescriptions) that indicates, reveals, or describes an individual's past, present, or future physical or mental health condition; provision of healthcare to an individual; or payment for the provision of healthcare. Data does not have to *identify* an individual to meet this definition. This restriction applies regardless of whether the transacting party is covered by HIPAA, and regardless of whether the data is encrypted, anonymized, or de-identified; or
6. Personal financial data (*e.g.*, information related to an individual's credit, debit cards, bank accounts, and financial liabilities, including payment history).

28 C.F.R. § 202.249(a)

C. Listed Personal Identifiers Defined

1. Full *or truncated* government identification or account numbers (*e.g.*, SSN, driver's license, passport, Alien Registration);
2. Full financial account numbers or PINs associated with financial institutions or financial services companies;
3. Device-based and hardware-based identifiers (*e.g.*, IMEI, MAC, SIM);
4. Demographic or contact data (*e.g.*, first and last name, date of birth, place of birth, ZIP code, residential address, telephone number, email address, or similar number);
5. Advertising identifier (*e.g.*, Google Advertising ID, Apple ID for Advertisers, mobile advertising identifiers);
6. Account-authentication data (*e.g.*, username, password, security question answers);
7. Network-based identifiers (*e.g.*, IP addresses, cookie data); and
8. Call-detail data (*e.g.*, Customer Proprietary Network Information).

28 C.F.R. § 202.234

D. Covered Personal Identifiers Defined

1. Any Listed Identifier combined with any other Listed Identifier; or
2. Any Listed Identifier combined with any other data disclosed by a transacting party pursuant to the transaction such that the Listed Identifier is linked, or linkable, to other Listed Identifiers *or to other sensitive personal data*.

But note that certain combinations are *excluded* from the definition of Covered Personal Identifiers:

1. Demographic or contact information linked *only* to other demographic or contact information; and
2. Account-authentication data, a network-based identifier, or call-detail data linked *only* to other account-authentication data, a network-based identifier, or call-detail data *as necessary* for the provision of telecommunications, networking, or similar service.

28 C.F.R. § 202.212

E. Exclusions

"Sensitive personal data" does *not* include:

1. Data that does not relate to an individual, such as a trade secret or proprietary information;
2. Data that is lawfully publicly available;
3. Personal communications; and
4. Information and informational materials and associated metadata needed to enable transmission. Such materials are limited to expressive materials and do not include technical functional, or otherwise non-expressive data.

28 C.F.R. §§ 202.249(b), 202.226

V. Transactions Subject to the Rule

"Covered transactions" include any transaction that involves any access by a CoC or CP to BUSPD or government-related data and that consists of data brokerage or a vendor, employment, or investment agreement.

A. Prohibited: Data Brokerage

"Data brokerage" refers to a type of data transaction, *not* a type of business. A business that is not primarily a "data broker" can still engage in this type of transaction. Data brokerage for the purposes of the rule consists of:

1. the sale of data,
2. licensing of access to data, or
3. similar commercial transactions

that involve the transfer of data from the *provider* to the *recipient* where the *recipient* did not collect or process the data directly.

The rule prohibits U.S. persons from engaging in data brokerage transactions with a CoC or CP where the transaction involves BUSPD or government-related data.

28 C.F.R. § 202.214, 202.243, 202.301

B. Onward Transfers: Data Brokerage

Although the rule generally applies to transfers of data or access from U.S. persons to CoCs or CPs, it adds a requirement to data brokerage transactions between U.S. persons and FPs who are *not* CoCs or CPs. U.S. persons engaging in such transactions must contractually require the FP not to engage in data brokerage transactions involving the same data with CoCs or CPs. U.S. persons must report known or suspected violations to DOJ within 14 days. And although DOJ has not provided guidance, it stated that, "At a minimum . . . U.S. persons must conduct sufficient due diligence to be able to comply with the reporting requirements, which could include periodic reviews with foreign counterparties to ensure that they have complied with the contract."

DOJ rejected proposals to exempt violations of onward transfer restrictions that are *de minimis*, made in good faith, or inadvertent.

28 C.F.R. § 202.302

C. Restricted: Vendor, Employment, and Investment Agreements

U.S. persons engaging in covered data transactions that involve vendor, employment, or investor agreements with a CoC or CP must comply with security requirements cross-referenced in the rule. U.S. persons engaging in such transactions should implement risk-based compliance programs, including record-keeping, to ensure and demonstrate compliance.

28 C.F.R. §§ 202.246, 202.401, 202.248

1. A "vendor agreement" is any agreement or arrangement in which a person provides goods or services to another person in exchange for payment or other consideration. Employment agreements are excluded from this definition.
2. An "employment agreement" is any agreement or arrangement in which an individual, other than as an independent contractor, performs work directly for a person in exchange for payment or other consideration. This includes board service.
3. An "investment agreement" is an 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 real estate in the United States or a U.S. legal entity. The rule excludes certain passive investments.

28 C.F.R. §§ 202.258, 202.217, 202.228

D. Exemptions

The rule exempts official U.S. government business, transactions required by U.S. law or U.S. international agreements (including Mutual Legal Assistance Treaties (MLATs), investment agreements that are subject to actions by the Committee on Foreign Investment in the United States (CFIUS), and certain de-identified or anonymized data related to regulatory authorization or approval of drugs, biological products, and medical devices.

Personal communications, information, and informational materials are exempt from the rule.

28 C.F.R. §§ 202.504, 202.507, 202.508, 202.510, 202.501, 202.502.

The rule also exempts data transactions that are "ordinarily incident" to the following activities. DOJ's examples and announcement of the rule make clear that such transactions must be incident to the referenced activities in the *ordinary* case to qualify for the exemption.

1. Travel, such as payment of living expenses, purchasing goods and services, and arranging transportation.

28 C.F.R. § 202.503

2. Financial Services, including online purchases of goods. The rule exempts data transactions that are ordinarily incident to and part of the provision of financial services such as banking, capital markets, financial insurance, and funds transfers.

The "financial services" exemption also exempts transfers of "personal financial data [and] 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)." This exemption applies to the purchase of all goods and services and is not limited to financial services.

28 C.F.R. § 202.505

3. Corporate Group Transactions. Corporate Group Transactions are transfers between a U.S. person company and a branch, affiliate, or subsidiary. A foreign "branch" of a U.S. company that is not separately organized under the laws of another country is still a U.S. person, and transactions with the foreign branch are not subject to the rule (although access by employees who are CPs would be).

If a subsidiary or affiliate is organized under the laws of a CoC or has its principal place of business there, it is a CP. Vendor agreements with that entity would be "restricted transactions" under the rule.

The rule exempts data transactions between a U.S. person and its CP subsidiary affiliate if those transactions are "ordinarily incident to and part of administrative or ancillary business operations." Examples include:

a. Human resources;

b. Payroll, expense monitoring and reimbursement, and other corporate financial activities;

c. Paying business taxes or fees;

d. Obtaining business permits or licenses;

e. Sharing data with auditors and law firms for regulatory compliance;

f. Risk management;

g. Business-related travel;

h. Customer support;

i. Employee benefits; and

j. Employees' internal and external communications.

DOJ's statements and examples make clear that, for a data transaction to qualify for the exemption, (a) the data transaction must be *incident* to a business operation; (b) the business operation must be *administrative or ancillary*; and (c) the data transaction must be *ordinarily* incident to such operations.

28 C.F.R. § 202.506

4. Telecommunications Services. Data transactions *other than data brokerage* that are ordinarily incident to and part of the provision of telecommunications services are exempt. Notably, DOJ expanded the definition of "telecommunications services" beyond the Telecommunications Act. For the purpose of the exemption, the definition is technology-neutral and includes, for example, communications services delivered over cable, Internet Protocol, wireless, fiber, and other transmissions mechanisms, as well as "arrangements for" network interconnect, transport, messaging, routing, or international voice, text, and data roaming.

DOJ rejected a proposal to exempt data transactions incident to the *function* of communications networks. DOJ concluded that such an exemption would functionally carve IP addresses out of the rule.

28 C.F.R. §§ 202.509, 202.252

5. Clinical Investigations and Post-Marketing Surveillance Data. Data transactions ordinarily incident to and part of clinical investigations that are regulated by the U.S. Food and Drug Administration (FDA) or that support applications to the FDA are exempt. Data transactions that are ordinarily incident to collection or processing of performance- or safety-related data or of post-marketing surveillance data and that are necessary to support or maintain FDA authorization are exempt as long as the data is de-identified or pseudonymized consistent with FDA regulations.

28 C.F.R. §§ 202.511

VI. Bulk Thresholds for Sensitive Personal Data

The rule only applies to data transactions involving U.S. sensitive personal data that exceeds a certain "bulk threshold." The rule defines "bulk" based on the thresholds below, and the rule's prohibitions and restrictions on data transactions involving BUSPD apply "regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted."

"Bulk" data is any amount of sensitive personal data that meets or exceeds the following thresholds at any point in the preceding 12 months:

Data Category	Bulk Threshold
Covered Personal Identifiers	100,000 U.S. persons
Personal Health Data	10,000 U.S. persons
Personal Financial Data	10,000 U.S. persons
Precise Geolocation Data	1,000 U.S. devices
Biometric Identifiers	1,000 U.S. persons
Human 'omic Data (not Genomic)	1,000 U.S. persons
Human Genomic Data	100 U.S. persons

Note that a data set that contains more than one cateogy is subject to the *lowest* threshold that applies to any category the data set contains.

These bulk thresholds do *not* apply to transactions involving government-related data. Government-related data is regulated regardless of its volume.

28 C.F.R. § 202.205

VII. Artificial Intelligence and Advertising

Considerations regarding artificial intelligence (AI) and advertising cut across sectors. The rule does not contain sections specific to artificial intelligence or advertising, but it discusses several examples of how the rule could apply to each. This may reflect an enhanced government interest in these two areas.

A. Artificial Intelligence and Training Data

The rule includes examples intended to highlight how the rule will "apply in certain scenarios where [BUSPD] would be licensed or sold to support algorithmic development . . . *or where sensitive personal data could be extracted from artificial intelligence models*." Examples include: the sale or licensing of BUSPD to a CP to develop AI/ML capabilities; providing a CP with access to BUSPD to develop an AI-based service or feature; licensing to a CP a chatbot trained on BUSPD that could *reproduce or disclose* that BUSPD if prompted; and licensing an AI algorithm in a manner that provides access to training data consisting of BUSPD.

B. Advertising

The Final Rule addresses the potential use of advertising IDs to reveal personal information about individuals. Examples of data transactions involving advertising include: providing location, IP address, and Ad ID data as part of the sale of advertising space in a mobile application and disclosure of BUSPD collected for the purpose of targeting advertising.

VIII. Rejected Proposals

For reference, DOJ rejected multiple proposals for modifications. These rejections may illuminate DOJ's objectives and threat assessment, which will likely inform enforcement priorities. Examples of proposals DOJ declined to adopt include:

- Exempting anonymized data.
- Exempting encrypted data, including data encrypted to post-quantum encryption standards.
- Exempting aggregated data.
- A consent-based exemption.
- A blanket exemption for third-party providers (relying instead on the "knowingly" standard).
- An exemption for product research, development, or improvement.
- An exemption for data transactions incident to the function of communications networks (DOJ concluded this would functionally exempt IP addresses).
- An exemption for transactions with contractual provisions retaining U.S. persons' direction and control over data processing.
- An exemption for transactions with contractual provisions requiring a CP to maintain privacy and secrecy of information.
- An exception to "onward transfer" liability for *de minimis* transfers, good faith, or inadvertent violations.
- A safe harbor for due diligence practices.

IX. Recommendations

U.S. businesses should assess whether they expose covered U.S. person- or U.S. government-related data to CoCs or to CPs. U.S. businesses should work with legal professionals to assess whether they engage in data transactions that implicate the rule and whether to implement risk-based compliance measures.

For example, U.S. companies may use customer service or back-end IT vendors overseas, or may have overseas branches that employ local nationals. Those arrangments may involve restricted transactions that need to be documented and mitigated. Medical and scientific research projects may need to be examined to determine whether they qualify for exceptions. DOJ's signaled areas of interest indicate that businesses in AI, mobile apps, and advertising sales should scrutinize their data flows and sharing practices to ensure conformity with the rule.

Our guidance on compliance and record-keeping is provided separately.