

February 2025

Follow us on [LinkedIn](#) 

Regulatory Update

DOJ and CISA Issue Final Rules Regulating Export of Bulk Sensitive Data

By [Aaron Charfoos](#), [Michelle Reed](#), [Keith Schomig](#), [Keith Feigenbaum](#), [Rachel Kurzweil](#), Nora Logsdon, Alex Sasse and [Shannon Sylvester](#)

The Department of Justice (DOJ) released a [Final Rule](#) restricting certain transfers of Americans' sensitive personal data to identified countries of concern or covered individuals. The Final Rule continues to assert the DOJ as a critical regulator of data transfers. In response to the rule, affected companies and individuals should establish robust compliance regimes and conduct due diligence and audits to prevent leakage of bulk sensitive personal data.

Background

On December 27, 2024, the DOJ announced its [Final Rule](#), implementing President Biden's Executive Order 14117 (the EO) of February 28, 2024, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern." On January 3, 2025, the U.S. Department of Homeland Security's Cybersecurity Infrastructure Security Agency (CISA) issued its [final security requirements](#) to implement the EO (collectively, the CISA Security Requirements).

The Final Rule was published in the Federal Register on January 8, 2025, and many of the provisions will become effective 90 days after publication (on April 8, 2025), though certain reporting, due diligence and auditing provisions will take effect in 270 days (on October 5, 2025).

The Final Rule follows the DOJ's earlier publication of a [Notice of Proposed Rulemaking](#) (NPRM) that builds on its Advanced Notice of Proposed Rulemaking (ANPRM) issued in March 2024. Additionally, CISA's final rules build on its previously released [Proposed Security Requirements for Restricted Transactions](#) under the EO (the Proposed Security Requirements).

Below, we have provided a summary of key takeaways for the DOJ's Final Rule and the CISA Security Requirements.

Key Takeaways

- The Final Rule regulates certain categories of prohibited and restricted transactions involving bulk sensitive personal data between U.S. persons and persons/entities with a nexus to specified countries of concern (namely China — including Hong Kong and Macau — Cuba, Iran, North Korea, Russia and Venezuela). “Bulk sensitive personal data” covers a broad range of sensitive personal data categories that meet established threshold amounts such as precise geolocation, personal health data, biometric identifiers, human ‘omic data, personal financial data and covered personal identifiers.
- Most of the provisions of the Final Rule take effect on April 8, 2025.
- The Final Rule has a broad scope and application, with implications for U.S. companies across various industries, and companies may face challenges in determining whether a transaction is a covered transaction and, if it is, whether it is prohibited or restricted.
- The Final Rule includes several exceptions to prohibited and restricted transactions, including travel and transactions “ordinarily incident to and part of the provision of” financial services or telecommunications services.
- Violations of the Final Rule could result in civil and criminal penalties.
- In concert with the release of the Final Rule, CISA released its final security requirements, which include updating asset inventories monthly, patching known exploited vulnerabilities within 45 days, implementing multifactor authentication on all covered systems, storing relevant logs for 12 months, including an allowlist by default, annually updating key policies and having detailed encryption requirements.

Summary of Key Provisions

Overall, the Final Rule generally follows the NPRM and seeks to prohibit or otherwise restrict certain transactions involving access to “bulk U.S. sensitive data” or “government-related data.” Specifically, as required by the EO, the Final Rule regulates “any transaction that involves any access by a country of concern or covered person to any government-related data or bulk U.S. sensitive personal data and that involves: (1) Data brokerage; (2) A vendor agreement; (3) An employment agreement; or (4) An investment agreement” (collectively, the covered transactions). These limitations generally apply to transactions between a U.S. person and a country of concern or a covered person, though the Final Rule provides some exemptions for certain transactions, as detailed below.

Countries of Concern

The term “country of concern” is defined as any foreign government that (1) has engaged in a long-term pattern or serious instances of conduct that threaten the security of the United States or U.S. persons and (2) poses a risk of exploiting government-related or bulk U.S. sensitive personal data at the expense of the U.S. national security. The same six countries discussed in the NPRM are identified as countries of concern: China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia and Venezuela.

Covered Persons

The Final Rule modified the definition of “covered person” from the NPRM. DOJ stated that this modification was intended to ensure consistency with the Department of the Treasury’s Office of Foreign Assets Control’s (OFAC) “50-percent rule language.” Under the Final Rule a “covered person” is:

- A foreign person that is an entity that is 50% or more owned, directly or indirectly, individually or in the aggregate, by one or more countries of concern or persons described in paragraph (a)(2) of Section 202.211; or that is organized or chartered under the laws of, or has its principal place of business in, a country of concern;
- A foreign person that is an entity that is 50% or more owned, directly or indirectly, individually or in the aggregate, by one or more persons described in paragraphs (a)(1), (3), (4) or (5) of Section 202.211;
- A foreign person that is an individual who is an employee or contractor of a country of concern or of an entity described in paragraphs (a)(1), (2) or (5) of Section 202.211;
- A foreign person that is an individual who is primarily a resident in the territorial jurisdiction of a country of concern; or
- Any person, wherever located, determined by the attorney general: (i) To be, to have been or to likely become owned or controlled by, or subject to the jurisdiction or direction of, a country of concern or covered person; (ii) to act, to have acted or purported to act, or to be likely to act for or on behalf of a country of concern or covered person; or (iii) to have knowingly caused or directed, or to be likely to knowingly cause or direct, a violation of this part.

As with the NPRM, the Final Rule includes several clarifying examples. Such examples make clear that the Final Rule exempts citizens of a country of concern if they primarily reside in a third country or in the United States, unless they are individually designated or employed by a country of concern or covered person. For example, a Russian citizen located in the United States is treated like a U.S. person. A Chinese citizen who primarily resides in a European Union country is also not a covered person, unless they are employed by a country of concern or a covered person. Examples of who would be considered a “covered person” include: (i) a foreign person located abroad and employed by a company that has been designated as a covered person; and (ii) a foreign person individual investor who principally resides in Venezuela and owns 50% of a technology company that is solely organized under the laws of the United States.

Notably, in responses to comments, the DOJ did advise that U.S. persons should continue to be mindful of “engaging in covered data transactions with an entity that is not a covered person but in which one or more covered persons have significant ownership that is less than 50%, or which one or more covered persons may control by means other than a majority ownership interest.” The DOJ specifically provides that ownership percentages can fluctuate such that an entity could become a covered person or be designated by the DOJ as a covered person in the future.

Covered Data: Bulk US Sensitive Personal Data and Government-Related Data

As with the NPRM, the Final Rule applies to covered data transactions involving “bulk,” “sensitive personal data” and certain “government-related data.”

Bulk Sensitive Data. The Final Rule regulates the transfer of certain sensitive, personal data if the data meets designated “bulk” volume thresholds, which the DOJ stated was based on a risk-based analysis, taking into account the threats, vulnerabilities and consequences associated with the data type. “U.S. sensitive personal data” means a collection, or set of sensitive personal data, relating to U.S. persons,

in any format, regardless of whether the data is anonymized, pseudonymized, de identified or encrypted, where such data meets or exceeds an established “bulk” threshold.

The Final Rule defines “sensitive personal data” as covered personal identifiers, precise geolocation data, biometric identifiers, human ‘omic data, personal health data, personal financial data or any combination thereof. Notably, the NPRM had included “human genomic data” rather than human ‘omic data, which is defined as human genomic data, human epigenomic data, human proteomic data and human transcriptomic data. The DOJ previously included nine potential categories of human ‘omic data in the NPRM and, in the preamble to the Final Rule, noted that it chose these three categories that posed the greatest risk because they “have the greatest clinical and predictive capacity, especially when used in combination with genomics and other ‘omic categories, because they are most closely related to genomics.”

“Bulk” means any amount of sensitive personal data, whether anonymized, pseudonymized, de identified or encrypted, that exceeds certain thresholds in the aggregate over the preceding 12 months before a “covered data transaction.” The Final Rule sets the following “bulk” thresholds:

Sensitive Data Category	Bulk Threshold
Human Genomic Data	Over 100 U.S. persons
Human ‘omic Data	Over 1,000 U.S. persons
Biometric Identifiers	Over 1,000 U.S. persons
Precise Geolocation	Over 1,000 U.S. devices
Personal Health Data	Over 10,000 U.S. persons
Personal Financial Data	Over 10,000 U.S. persons
Certain Covered Personal Identifiers	Over 100,000 U.S. persons

The definition of “bulk” also include “combined data,” which means any collection or set of data that contains more than one of the above listed categories, or that contains any listed identifier linked to human ‘omic data, biometric identifiers, precise geolocation, personal health data and personal financial data, where any individual data type meets the threshold number of persons or devices collected or maintained in the aggregate for the lowest number of U.S. persons or U.S. devices in that category of data.

Note that in a change from the NPRM, which listed “human genomic data” as a category, the Final Rule changed the reference to “human ‘omic data.”

Government-Related Data. The Final Rule strictly limits transfer of government-related data, regardless of volume. No government-related data of any amount may be transferred to a covered person or country of concern. The Final Rule defines two categories of government-related data: data related to locations of government activities and data on U.S. government personnel.

Prohibited Transactions

The Final Rule defines specific categories of prohibited transactions with a country of concern or covered person.

Data-Brokerage Transactions. The Final Rule prohibits a U.S. person from engaging in a covered transaction involving data brokerage with a country of concern or a covered person. A “data brokerage” means 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. The Final Rule provides several clarifying examples, such as:

- A U.S. organization maintains a database of bulk U.S. sensitive personal data and offers annual memberships for a fee that provide members a license to access that data. Providing an annual

membership to a covered person that includes a license to access government related data or bulk U.S. sensitive personal data would constitute prohibited data brokerage.

- 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, the U.S. company 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 12-month period. 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.
- A U.S. company owns or operates a mobile app or website for U.S. users. That mobile app or website contains one or more tracking pixels or software development kits that were knowingly installed or approved for incorporation into the app or website by the U.S. company. The tracking pixels or software development kits transfer or otherwise provide access to government-related data or bulk U.S. sensitive personal data to a country of concern or covered person-owned social media app for targeted advertising.

Similar to the NPRM, the Final Rule also prohibits a U.S. person from knowingly engaging in any transactions involving the potential onward transfer of such data to countries of concern or covered persons. Specifically, a U.S. person transacting with noncovered foreign persons must contractually prohibit the subsequent transfer of sensitive personal data or government-related data to a country of concern or covered person and report any known or suspected violations of this contractual requirement. The DOJ indicated that it anticipates forthcoming compliance and enforcement guidance that will provide model contractual language to satisfy this requirement.

Human 'Omic Data and Human Biospecimen Transactions. The Final Rule prohibits a U.S. person from knowingly engaging in any covered data transaction with a country of concern or covered person that involves access by that country of concern or covered person to bulk U.S. sensitive personal data that involves bulk human 'omic data, or to human biospecimens from which bulk human 'omic data could be derived.

Other Prohibited Transactions. The Final Rule also prohibits a transaction that is meant to evade, avoid, violate or attempt to violate the Final Rule's prohibition on transfers and from knowingly directing prohibited a prohibited transaction or noncompliant restricted transaction.

Restricted Transactions

Like the NPRM, the Final Rule includes certain transactions that are "restricted," instead of wholly prohibited. Restricted transactions include covered data transactions that involve a vendor agreement, employment agreement or investment agreement with a country of concern or covered person. U.S. persons may only engage in such transactions if they satisfy the Final Rule's compliance obligations, including the CISA Security Requirements, discussed in detail below.

Third-Party Platforms

The Final Rule clarifies that U.S. persons providing third-party platforms or infrastructure are not civilly or criminally responsible for their customers' prohibited or restricted transactions on those platforms. They are only responsible for the prohibited or restricted transactions that they conduct.

Exempt Transactions

The Final Rule exempts the same transactions as previously listed in the NPRM and provides illustrative examples. Specifically, the Final Rule exempts:

- *Personal Communications*: Data transactions that involve any postal, telegraphic, telephonic or other personal communication that does not involve the transfer of anything of value.
- *Information or Informational Materials*: Data transactions that involve the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or informational materials.
- *Travel*: Data transactions that are ordinarily incident to travel to or from any country, including importation of accompanied baggage for personal use; maintenance within any country, including payment of living expenses and acquisition of goods or services for personal use; and arrangement or facilitation of such travel, including nonscheduled air, sea or land voyages.
- *Official Business of the U.S. Government*: Data Transactions that are for the conduct of the official business of the United States government by its employees, grantees or contractors; any authorized activity of any United States government department or agency (including an activity that is performed by a federal depository institution or credit union supervisory agency in the capacity of receiver or conservator); or transactions conducted pursuant to a grant, contract or other agreement entered into with the United States government.
- *Financial Services*: Data transactions that are ordinarily incident to a part of the provision of financial services, including:
 - Banking, capital markets (including investment management services as well as trading and underwriting of securities, commodities and derivatives), or financial insurance services;
 - A financial activity authorized for national banks by 12 U.S.C. 24 (Seventh) and rules, regulations and written interpretations of the Office of the Comptroller of the Currency thereunder;
 - Activities that are “financial in nature or incidental to such financial activity” or “complementary to a financial activity,” Section (k)(1), as set forth in Section (k)(4) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)(4)) and rules and regulations and written interpretations of the Board of Governors of the Federal Reserve System thereunder;
 - 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 (such as services for payment dispute resolution, payor authentication, tokenization, payment gateway, payment fraud detection, payment resiliency, mitigation and prevention and payment-related loyalty point program administration); and
 - The provision of investment management services that manage or provide advice on investment portfolios or individual assets for compensation (such as devising strategies and handling financial assets and other investments for clients) or provide services ancillary to

investment management services (such as broker-dealers or futures commission merchants executing trades within an investment portfolio based upon instructions from an investment advisor).

- *Corporate Group Transactions*: Data transactions that are between a U.S. person and its subsidiary or affiliate located in (or otherwise subject to the ownership, direction, jurisdiction or control of) a country of concern and ordinarily incident to and part of administrative or ancillary business operations, including:
 - Human resources;
 - Payroll, expense monitoring and reimbursement and other corporate financial activities;
 - Paying business taxes or fees;
 - Obtaining business permits or licenses;
 - Sharing data with auditors and law firms for regulatory compliance;
 - Risk management;
 - Business-related travel;
 - Customer support;
 - Employee benefits; and
 - Employees' internal and external communications.
- *Transactions Requirement by Law or Treaty*: Data transactions that are required or authorized by federal law or pursuant to an international agreement to which the U.S. is a party.
- *Committee on Foreign Investment in the United States (CFIUS)*: Data transactions that involve an investment agreement that is subject to a CFIUS action.
- *Telecommunications Services*: Data transactions, other than those involving data brokerage, that are ordinarily incident to and part of the provision of telecommunications services. Notably, the Final Rule expanded the definition of "telecommunications service" to include voice and data communications over the internet in addition to services that meet the definition in 47 U.S.C. 153(53).
- *Life Sciences Authorizations*: Data transactions involving drug, biological product, device or combination product approvals or authorizations if the data transactions involve "regulatory approval data" necessary to obtain or maintain regulatory approval. "Regulatory approval data" means sensitive personal data that is de-identified or pseudonymized consistent with FDA regulations and required by a regulatory entity to research or market a drug, biological product, device or combination product, including postmarketing studies and surveillance. It excludes data not reasonably necessary for assessing safety and effectiveness. The terms "drug," "biological product," "device" and "combination product" have the meanings set forth in 21 U.S.C. § 321(g)(1), 42 U.S.C. § 262(i)(1), 21 U.S.C. § 321(h)(1) and 21 CFR § 3.2(e). The Final Rule expanded and clarified several pieces of this exemption from the NPRM. For example, the NPRM previously limited this exemption to only those transactions necessary to obtain or maintain approval to market a drug, biological product or device.

- **Clinical Investigations and Postmarketing Surveillance Data:** Transactions that are part of clinical investigations regulated by the FDA, or support FDA applications for research or marketing permits for drugs, biological products, devices combination products or infant formula, and the data are de-identified or pseudonymized consistent with FDA regulations (21 C.F.R. 314.80(i)). Such transactions are also exempt if they are part of the collection or processing of clinical care data indicating real-world performance or safety of products, or postmarketing surveillance data necessary to support or maintain FDA authorization, provided the data is de-identified or pseudonymized.

The Final Rule also exempts transactions data that is lawfully publicly available from government records or widely distributed media (like freely available, open-access repositories) and metadata that is ordinarily associated with expressive materials, or that is reasonably necessary to enable the transmission or dissemination of expressive materials (such as geolocation data embedded in digital photographs).

License Program

As with the NPRM, the Final Rule authorizes the DOJ to grant general licenses for categories of transactions that might otherwise be restricted or prohibited under specified conditions. Such transactions will not require further authorization. Additionally, the Final Rule creates a mechanism for parties to apply for specific licenses for specific transactions. The Final Rule sets out the requirements and procedures for both the general and specific license, including a process for applying for a specific license and the reconsideration of denied licenses. Separate instructions from the DOJ on specific licenses are forthcoming.

Guidance and Advisory Opinions

Like the NPRM, the Final Rule provides that U.S. persons can request an advisory opinion from the attorney general and DOJ, but they must disclose the details of an actual, not hypothetical, transaction. The department may respond with its present enforcement intent, it can decline to state its intent or it can provide comments to the parties. The parties can withdraw their request, but they can only do so before an advisory opinion is issued.

The Final Rule also permits the DOJ to issue general public guidance to address frequently asked questions and common issues.

Compliance Requirements and Reporting Requirements

The Final Rule does not contain general compliance requirements for all U.S. persons or companies engaged in international data transactions. Instead, the Final Rule expects U.S. companies to develop and implement compliance programs based on their own risk profiles.

However, like the NPRM, the Final Rule, establishes a number of compliance requirements for U.S. persons and companies engaged in prohibited and restricted transactions with covered persons and countries of concern. The requirements include due diligence, audits, recordkeeping and reporting as well as implementing a comprehensive compliance program that includes risk-based procedures to verify and log data flows, sensitive personal and government-related data types and volume, transaction parties' identities, data end-use and transfer methods, and vendor identities. Additionally, such requirements include establishing written policies on data security and compliance that are certified annually by a responsible officer or employee, and conducting and retaining the results of an annual audit by an internal or external independent auditor to verify compliance with the CISA Security Requirements.

The Final Rule also requires that all parties engaged in covered transactions keep records of each transaction and a record of their data compliance, and that the records be available for examination for at least 10 years. The DOJ may request reports on any of the compliance requirements at any time, and U.S. persons involved in covered transactions must independently submit annual reports to the DOJ. If a

U.S. person rejects a transaction because it violates a prohibition of the Final Rule, that person must also report the transaction to the DOJ.

The Final Rule clarifies that companies can use existing audits, reports and other compliance practices as long as they meet the requirements of this rule, and thus there is no need to create duplicative or separate systems or reports, and that U.S. persons may use either internal or external audits so long as they are independent and meet the other requirements of the rule. Further, the Final Rule notes that audits for restricted transactions need only review a U.S. person's restricted transactions and only relevant policies, personnel and systems.

Enforcement

Under the Final Rule, the DOJ can investigate violations of the proposed rule and impose civil or criminal penalties. Like other International Emergency Economic Powers Act programs, when imposing civil penalties, the department must file prepenalty notice and give the alleged violator the opportunity to respond and begin settlement negotiations.

Civil penalties cannot exceed \$368,136, or an amount twice the amount of the violative transaction. Criminal penalties cannot exceed \$1,000,000, imprisonment for up to 20 years or both.

Coordination With Other Agencies and Regulations

CFIUS

The DOJ's Final Rule follows the approach outlined in the proposed rule, which exempts investment agreements that are subject to a CFIUS action that relates to sensitive personal data. A CFIUS action includes CFIUS issuing an interim order, the parties entering into a mitigation agreement or CFIUS imposing a condition with respect to a particular covered transaction under the Final Rule. This allows the Department of the Treasury, as the lead agency for CFIUS reviews, to retain its authority over violations of the proposed rule if they are subject to CFIUS jurisdiction. If CFIUS does not have jurisdiction or is requesting information about a transaction in a "non-notified" instance, the DOJ will work with the Department of the Treasury to enforce compliance with the Final Rule.

An investment agreement that is both a "restricted transaction" under the Final Rule and a "covered transaction" under CFIUS is still subject to the security requirements until the transaction is filed with, and action is taken by, CFIUS. The Final Rule contains examples to help clarify this double requirement. In example four of § 202.508, a U.S. manufacturer is acquired by a foreign owner and the parties enter into a mitigation agreement to resolve supply assurance concerns in the interest of national security. There are no provisions in the mitigation agreement that address data security. This transaction and mitigation agreement would not be considered a CFIUS action within the meaning of the Final Rule and the transaction would still be subject to the Final Rule.

The Final Rule regulates a broad set of transactions to supplement CFIUS's voluntary, case-by-case approach with generally applicable rules. Under the Final Rule, when a covered transaction also involves an investment covered by CFIUS, the Final Rule's security requirements for restricted transactions would apply until CFIUS takes action. Once CFIUS has taken action, the investment agreement would become exempt from the Final Rule and only be subject to CFIUS's authority. In cases where CFIUS did not review a particular transaction or take a CFIUS action, obligations under the Final Rule would continue to apply with respect to the transaction. CFIUS could also refer a covered transaction to the president, after which the Final Rule would continue to apply while the DOJ and Department of Treasury coordinated on any enforcement actions.

FTC

Despite comments related to potential overlap between the rule and the Protecting Americans' Data from Foreign Adversaries Act of 2024 (PADFAA), which is enforced by the Federal Trade Commission, the DOJ declined to alter the rule with respect to potential interaction with PADFAA. In consultation with the FTC, the department concluded that PADFAA varies significantly from the rule. For example, PADFAA applies only to entities defined as "data brokers," whereas the Final Rule regulates "data brokerage" transactions and covers a broader range of activities and entity types. In addition, the rule covers U.S. persons while PADFAA covers only "entities." The Final Rule also addresses additional risks, including the resale of data by third parties and indirect sales through intermediaries. The rule provides mechanisms for clarification and redress, including through advisory opinions, general licenses and specific licenses, which PADFAA lacks. Finally, the rule utilizes different criteria to designate "covered" persons under the program. The DOJ intends to coordinate with the FTC in the future to minimize conflicting or duplicative enforcement.

Department of Commerce

Vendor agreements covered under the Final Rule could also potentially be subject to Department of Commerce actions related to information and communications technology and services (ICTS) transactions under Executive Orders 13873 and 14034. Despite this potential for overlap with the Department of Commerce's authority, the DOJ decided not to change the scope of the Final Rule from that proposed in the NPRM. While both authorities address similar national security risks related to vendor agreements, each focuses on different vectors of risk. Executive Orders 13873 and 14034 specifically address the acquisition, import or use of technology developed or sourced from a foreign adversary in the United States or by U.S. persons. The Final Rule, on the other hand, seeks to address transactions involving the export of U.S. sensitive personal data by, for example, prohibiting a U.S. person from entering into a vendor agreement that allows countries of concern or covered persons access to bulk U.S. sensitive personal data.

CISA Security Requirements

As directed by EO 14117, CISA has developed the following security requirements to apply to classes of restricted transactions identified in regulations issued by the DOJ. CISA's requirements impose conditions specifically on the covered data that may be shared as part of a restricted transaction; on the covered systems more broadly; and on the organization as a whole. Note that the security requirements define covered system broadly as any information system used to obtain, read, edit, collect, decrypt, etc. conveyed data that is part of a restricted transaction.

Organizational and System-Level Requirements

At the organizational and system-level, the security requirements state that covered systems must institute basic cybersecurity policies. All data, systems and facilities must be identified, documented and updated on a regular basis. Organizations should designate an individual to be responsible for cybersecurity and compliance functions. The requirements also state that organizations should institute a remediation plan in the event of a breach, document IT and cybersecurity vendors and suppliers, and implement a technology audit and approval process.

The security requirements direct covered systems to develop access controls to prevent unauthorized persons from gaining access to covered sensitive personal data or government-related data. Companies must enforce multifactor authentication, revoke access of employees who have changed positions or have left the organization and track any access- or security-related events in the covered system. The requirements note that organizations must maintain policies to prevent unauthorized connections to the covered system. Further, organizations should conduct and document an annual data risk assessment to ensure compliance with these requirements.

Data-Level Requirements

CISA requires that a combination of the data-level requirements should be implemented in the way that best prevents access to covered data by covered persons and countries of concern. The requirements suggest applying data minimization strategies such as maintaining a data retention and deletion policy and processing the data in a way that makes it noncovered or nonlinkable data. Companies should also apply encryption techniques as outlined in the NIST Privacy Framework and privacy enhancing technologies to process covered data.

Looking Ahead

Companies and entities that may be subject to the Final Rule should take steps to prepare for when the rule comes into effect in April and October this year. While we anticipate further guidance from the DOJ, covered entities can take the following steps to prepare:

- **Data Mapping.** Review or conduct an inventory of the data that the entity is processing and where data may be transferred to.
- **Review Data Transfers.** Review existing agreements and related transactions, including intragroup transfers, vendor agreements, employment agreements and investment agreements that involve the transfer of personal data, to determine whether such transactions are in scope of the Final Rule. Companies should also begin to prepare contingencies should vendors need to be replaced, or new data storage locations found.
- **Review and Revise Contracts.** Review applicable agreements and determine whether they need to be revised to address requirements for the Final Rule, including any restrictions on onward transfers.
- **Update Compliance and Security Programs.** Companies should review and revise compliance programs to address the requirements of the Final Rule as well as the CISA Security Requirements. Companies should understand (1) the types of information they collect, (2) the entities or individuals to which they sell or with whom they share that information and (3) the entities or individuals involved in data collection and processing, and update their compliance programs accordingly.

The Paul Hastings Data Privacy and Cybersecurity and Global Trade Controls practices regularly advise on related matters and are closely monitoring developments related to the Final Rule. If you have any questions concerning how the Final Rule may affect your organization, please do not hesitate to contact any member of our teams.



If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Chicago

Aaron Charfoos
+1-312-499-6016
aaroncharfoos@paulhastings.com

Dallas

Michelle A. Reed
+1-972-936-7475
michellereed@paulhastings.com

Washington, D.C.

Keith Schomig
+1-202-551-1880
keithschomig@paulhastings.com

Keith Feigenbaum
+1-202-551-1929
keithfeigenbaum@paulhastings.com

Rachel Kurzweil
+1-202-551-1940
rachelkurzweil@paulhastings.com

Nora J. Logsdon
+1-202-551-1772
noralogsdon@paulhastings.com

Alex Sasse
+1-202-551-1749
alexsasse@paulhastings.com

Shannon P. Sylvester
+1-202-551-1797
shannonsylvester@paulhastings.com

Paul Hastings LLP

Stay Current is published solely for the interests of friends and clients of Paul Hastings LLP and should in no way be relied upon or construed as legal advice. The views expressed in this publication reflect those of the authors and not necessarily the views of Paul Hastings. For specific information on recent developments or particular factual situations, the opinion of legal counsel should be sought. These materials may be considered ATTORNEY ADVERTISING in some jurisdictions. Paul Hastings is a limited liability partnership. Copyright © 2025 Paul Hastings LLP.