Davis Polk

DOJ finalizes rule restricting sensitive data transfers to countries of concern, including China

January 23, 2025 | Client Update | 38-minute read

Beginning in April 2025, the new rule will require many U.S. companies to adopt government-imposed cybersecurity standards before entering into, or prohibit altogether, a wide range of transactions giving persons and entities linked to countries of concern access to sensitive U.S. data. The new requirements are based on perceived national security threats, not privacy, and apply to existing and internal relationships as well as new transactions.

On December 27, 2024, the Department of Justice (DOJ) issued a final rule that aims to prevent access to Americans' bulk sensitive personal data and U.S. government-related data by "countries of concern," including China. The final rule prohibits transactions by U.S. companies in which significant quantities of sensitive personal data are transferred to China-linked companies outside the United States and conditions a wide range of employment, investment, and procurement transactions with those companies on compliance with a series of cybersecurity requirements released in parallel by the Cybersecurity & Infrastructure Security Agency (CISA) and reproduced below as Appendix B. The rule will become effective on April 8, 2025 and does not contain any exemptions for pre-existing contracts, meaning that continued access to sensitive data under current vendor, employment, and commercial relationships will be affected. "Sensitive data" includes a broadly defined set of health, financial, geolocation, and personally identifying information of U.S. persons.

The rule reflects a growing concern that countries of concern, including China, could (or already do) use sensitive data to undermine national security by identifying vulnerabilities, conducting espionage or exposing U.S. citizens and officials to manipulation and blackmail. Under the outgoing administration, DOJ articulated the view that such sensitive data risks are an increasingly urgent national security gap, and DOJ rushed to put the rule in place before the transition to a new administration. The rules were mandated by Executive Order 14117, issued by President Biden in February 2024 with a concurrent advanced notice of proposed rulemaking (ANPRM). Detailed rules were proposed in a notice of proposed rulemaking (NPRM) in October, which we discussed in this client update, and finalized with minimal change following a comment period of only thirty days. A number of important points of ambiguity remain. DOJ has suggested that, in the short term, it may provide additional guidance or certain forms of relief, such as a temporary wind down general license.

U.S. companies will soon be expected to comply with the broad and complex regulatory scheme envisioned by the new rule. Firms will also have until October 2025 to develop required due diligence, reporting and auditing processes required by the rule. Nevertheless, challenges remain for businesses seeking to interpret the rule and adhere to new requirements affecting a wide range of commonplace and crucial transactions with China-based or Chinese-owned vendors, employees, customers, and investors—including a company's own affiliates.

Summary of the final rule

The rule applies two sets of requirements to U.S. persons and companies engaging in transactions with **covered persons**, which are foreign persons or entities located in or owned by residents of **countries of concern** (China, Russia,

Copyright 2025 Davis Polk & Wardwell LLP

Cuba, Iran, North Korea and Venezuela), that could provide access to broad categories of **bulk U.S. sensitive personal data** or **government-related data** (Covered Data). The thresholds for "bulk" data can be quite low (as few as 100 individuals for genomic and similar data, and there is no quantitative threshold at all if sensitive personal data is marketed as specific to government employees), and anonymization alone does not remove data from the scope of the rule. The rule does not restrict data collection or use by U.S. persons (generally including U.S. companies that may themselves be owned by persons of a country of concern). Nor does the rule restrict transactions with foreign persons that are not covered persons (i.e., not linked to countries of concern) absent certain indications of evasion.

- **Prohibited transactions:**
  - U.S. persons may not knowingly engage in **data brokerage** transactions with covered persons. As discussed below, "data brokerage" is defined broadly to cover many commercial transactions involving transfers of Covered Data, even where such transfer is not the primary purpose of the transaction (e.g., transfers of customer information in connection with the sale of a line of business).
  - U.S. companies holding any significant quantity of **human 'omic data** (genomic and other data defined below) on U.S. persons may not knowingly engage in investment, employee, or vendor relationships with the potential to provide access to such data to a covered foreign person.
- **Restricted transactions:**
  - Before knowingly engaging in any **investment agreement**, **employment agreement** or **vendor agreement** in which a covered person will have access to Covered Data, U.S. persons and companies holding Covered Data must meet the data security requirements promulgated by CISA; until the standards are satisfied, the transaction is prohibited. An **investment agreement** involving potential access by a person of a country of concern to any Covered Data is subject to such data security requirements unless the investment is in publicly traded securities of the issuer, amounts to a total of less than 10% of the U.S. business, and is completely passive. Although the rule is not entirely clear, it appears that all investments not meeting the size and passivity criteria are conclusively presumed to provide potential access to Covered Data.

Any foreign person primarily resident in a country of concern is a covered person. Foreign entities are covered persons if organized, located in, or controlled by a country of concern. U.S. persons must conduct sufficient diligence (both on the data they themselves hold and on their potential counterparties) to determine whether restrictions or prohibitions apply. The rule operates with a constructive knowledge standard that requires U.S. persons to conduct risk-based diligence on potential counterparties. As with sanctions administered by the Office of Foreign Assets Control (OFAC), U.S. persons will be able to seek specific licenses under the rule. There are a number of exemptions to the rule's restrictions and prohibitions, including for transactions incident to the ordinary provision of financial services or telecommunications services.

U.S. persons must comply with the rule beginning on April 8, 2025, although the effective date of some diligence and recordkeeping requirements has been delayed until October 6, 2025. The final rule clarifies that all transactions involving Covered Data following the effective date of the rule are covered, even if access to data is provided pursuant to an agreement entered into prior to the effective date. The DOJ is considering issuing a wind down license that would allow time for amendment of contracts signed before the effective date, but at present such relief is not available.

Detailed discussion of the rule

Foreign persons targeted

The rule only applies to transactions that could provide access to sensitive data to a **covered person**, which is generally defined as any foreign person that is:

- an entity that is 50% or more owned, directly or indirectly, individually or in the aggregate, by a country of concern, or that is organized or chartered under the laws of, or has its principal place of business in, a country of concern;
- a foreign individual who is an employee or contractor of a country of concern or of an entity that is a covered person;
- a foreign individual who is primarily a resident in the territorial jurisdiction of a country of concern (note that the test is residency, not citizenship); or
- a foreign entity that is 50% or more owned, directly or indirectly, individually or in the aggregate, by any of the foregoing or designated covered persons.

Copyright 2025 Davis Polk & Wardwell LLP

The preamble to the final rule made clear that the 50% ownership threshold is intended to function similarly to OFAC's "50% rule," including by aggregating all ownership of covered persons, covered or not, to determine whether the threshold is reached. Once 50% is reached, the entity is itself a covered person, such that a 50% subsidiary of a 50% subsidiary is also a covered person. (Conversely, although the final rule does not state this explicitly, under OFAC practice an entity with less than 50% ownership by covered persons is disregarded, so that indirect ownership is not attributed pro rata to minority shareholders.)

The definitions above exclude U.S. citizens, U.S. nationals, lawful permanent residents, lawful refugees and asylum grantees (regardless of their country of residence); entities organized solely under U.S. law (including foreign branches of U.S. companies without separate legal personality, but not foreign subsidiaries, as well as U.S. entities owned by covered persons); and foreign persons or entities physically within the United States. However, U.S. persons (and other entities) may be affirmatively designated as covered persons by the Attorney General because, among other reasons, they are owned by, controlled by, or acting on behalf of covered persons; these persons will be named on a publicly available list (similar to sanctions lists).

The initial list of countries of concern consists of China, Russia, Iran, North Korea, Cuba and Venezuela. The Attorney General, with the concurrence of the Secretary of State and Secretary of Commerce, may designate additional countries of concern in the future.

U.S. persons required to comply

Only U.S. persons (as defined above) are required to comply with the rule. They are also prohibited from knowingly directing a foreign person to engage in a transaction that would be prohibited for a U.S. person, either because they have authority to make decisions for or on behalf of an entity (so, for example, an officer or senior director who approves a transaction, but not an accounting employee who processes a payment) or because they engage the entity as an intermediary.

Transactions among non-U.S. persons are therefore generally not covered; however, the rule has certain collateral consequences for transactions even solely among non-U.S. persons:

- The prohibition against directing an impermissible transaction may apply to a U.S. person senior employee of a non-U.S. company; recusal may be necessary.
- U.S. persons engaged in data brokerage transactions with foreign persons that are not covered persons are required to include contractual provisions prohibiting onward sale of the data to covered persons, which may expose the original buyer to liability in case of violations.

Covered data

The rule applies to two different types of data: bulk U.S. sensitive personal data and government-related data.

Bulk U.S. sensitive personal data

The rule defines "**sensitive personal data**" to include **precise geolocation data** (with "precise" being defined as "within one kilometer"), **biometric identifiers**, **human 'omic data**, **personal health data**, and **personal financial data**. The term also encompasses **covered personal identifiers**, meaning a specific list of commonplace identifiers that includes government ID numbers such as Social Security Numbers, demographic or contact data (such as name, birthdate, telephone number, or e-mail and street addresses), and advertising-related digital identifiers that could be used to identify an individual from a dataset or to link or make a listed identifier linkable across multiple datasets to an individual. "Human 'omic data" is an expansion of the NPRM's coverage of "human genomic data" to include epigenomic, proteomic, and transcriptomic data, which the DOJ determined are related and quickly developing fields that also have potential for identification of individuals or other malicious uses. The rule also covers human biologic samples from which such data can be derived.

Stand-alone lists of single personal identifiers, or demographic or contact information linked only to other demographic or contact information, are not bulk U.S. sensitive personal data unless the identifier is linkable[1] to another listed identifier or sensitive personal data based on other data disclosed by a transacting party.[2] For example, a telephone directory is not a covered personal identifier, but if a company sells a list of Media Access Control addresses *and* tells the recipient those addresses connected to the wifi network of a restaurant in a government building, the additional information disclosed about the location of the restaurant, even though in a different format and unstructured, would make the addresses linkable to precise geolocation data of individuals frequenting the same restaurant.[3] The rule also excludes personal

Copyright 2025 Davis Polk & Wardwell LLP

identifiers that are only linked to other identifiers

Importantly, data that has been anonymized or encrypted **is** within the scope of the rule. Compliance with CISA's standards, which may include anonymization and encryption, can make a transaction that would otherwise be prohibited permissible, but the CISA standards must be complied with as a whole, and anonymization does not itself render data not covered. Anonymous genetic sequences or tissue samples of U.S. persons, for example, are covered data.

The rule only applies restrictions to transactions over specified "bulk" thresholds, which are determined based on the total volume of data transacted over the preceding 12 months. The thresholds vary depending on the type of data involved, as detailed in Appendix A.

U.S. government-related data

Government-related data comprises two categories of data:

- **Precise geolocation data** for devices or individuals in any location within one of the areas listed on the Government-Related Location Data List included in the rule. The list expanded significantly from the NPRM and now covers more than 700 areas in the United States defined by geocoordinates, and additional areas may be added by the Attorney General in the future.
- **Sensitive personal data**, regardless of volume, that is *marketed* as linked or linkable to current U.S. government employees or contractors, recent former employees or contractors, or former senior officials.[4]

Covered data transactions

The rule restricts or prohibits four types of transactions—as opposed to the general collection or storage of data—that "involve[ ] any **access** by a country of concern or covered person" to Covered Data. The definition is pragmatic rather than formalistic, and an actual export of data to the country of concern is not required. If there is no possibility of access to such data, the transaction is not covered even if it falls in one of the four categories (but see below with respect to investment agreements). Conversely, if there is a realistic possibility of access to Covered Data, contractual safeguards alone are unlikely to remove the transaction from the scope of the rule.

- **Data brokerage:** The sale of data, licensing of access to data, or similar commercial transactions involving the transfer of data to a person who did not collect or process the data directly from the individuals linked or linkable to the data.
  - Data brokerage may include not only stand-alone sales of data, but sales or licensing of data in connection with bona fide commercial transactions (e.g., if in selling advertising space advertising IDs are provided in bulk). Vendor, employment, or investment agreements, however, will not be considered "data brokerage" (i.e., the categories are intended to be mutually exclusive).
  - E-commerce activities, such as providing personal identifiers in the process of paying for goods and services, while potentially falling in this category, would generally be covered by the exemption (below) for financial services.
  - As discussed below, a U.S. person must have at least constructive knowledge that data is being passed to a covered foreign person, so a file sharing site would not engage in data brokerage merely because two other parties used it to exchange information.
  - However, U.S. persons engaged in data brokerage with foreign persons who are **not** covered persons must include a contractual prohibition prohibiting onward sale to a covered person and report any violation.

  According to the final rule, "data brokerage" requires some form of compensation, and the final rule repeatedly asserts that data transfers without payment, such as research collaborations, are not covered. However, the final rule also gives, as an example of a covered transaction, unpaid service on a nonprofit board giving access to Covered Data, because the prestige and experience of serving on the board is a form of compensation (a rationale that would seem to apply equally to research collaborations). The contradiction is not resolved.

- **Vendor agreement**: Any arrangement, other than an employment agreement, for providing goods or services to another person for consideration, including cloud computing services, involving access to covered data.
- **Employment agreement**: Any arrangement for an individual, other than as an independent contractor, to perform work or job functions directly for a person in exchange for consideration, if the arrangement involves access to covered data. Paid board service is considered an employment agreement.

Copyright 2025 Davis Polk & Wardwell LLP

– **Investment agreement**: Any arrangement to obtain direct **or** indirect ownership interests in or rights in relation to (1) real estate located in the United States or (2) a U.S. legal entity in exchange for consideration involving access to covered data. As noted, there is **no** exception for pre-existing agreements, meaning that the exercise of existing rights such as options or pre-emptive rights, or meeting obligations such as capital calls, is within the scope of the rule.

  Passive investments that provide a covered person with less than 10% total voting and equity interests in a U.S. person, that do not afford any special rights other than standard minority shareholder protections, and that are investments in publicly-traded securities, SEC-registered funds, or private pooled investment funds are not covered transactions. All three conditions (passivity, publicly-traded security or LP investment, and less than 10% by vote and value) must be met.

  There are, however, some critical ambiguities in the investment agreement definitions.

  - Most importantly, the "covered data transaction" definition only covers "any transaction that involves any access by a country of concern or covered person" to Covered Data. The discussion of "investment agreements" makes the non-controversial point that whether that access is pursuant to (or even in contravention of) the parties' contractual rights is irrelevant. However, one of the examples given appears to conclusively presume that any investment that does not satisfy all three conditions (for example, acquiring even a single share in a private company) *necessarily* involves access to any Covered Data held by the U.S. company and is subject to the rule's prohibitions without spelling out the analysis. If it is factually untrue that a minority investment affords any access or ability to access Covered Data, it seems that the investment would not meet the "covered data transaction" definition set out in the rule, but it appears that DOJ may disagree.
  - Also, DOJ added the private equity exemption for passive investments of 10% or less in the final rule. However, a U.S. private equity fund is, by definition, not a covered person, nor is a non-Chinese foreign private equity fund that is less than 50% owned by covered persons, and so it would seem that U.S. person investment transactions with those funds would not be covered (any more than any other legal entity that did not meet the ownership tests). The logical reading would be that a U.S. private equity fund that held, through portfolio companies, bulk sensitive personal data could not enter into or execute investment agreements with covered persons that did not qualify for the 10% and passive exemption, but the intent is not entirely clear.

Prohibitions and restrictions

Prohibited transactions

The rule would prohibit any U.S. person from knowingly engaging in or directing certain categories of covered data transactions with a covered foreign person absent a license. In particular, covered data transactions with covered persons or countries of concern involving **data brokerage** or involving the **bulk transfer of human 'omic data** (including investment transactions, so that significant investments by covered persons in U.S. companies holding any significant quantity of genomic data would be prohibited) or biospecimens from which data can be derived would be prohibited absent a license.

Restricted transactions

All other covered data transactions with covered persons or countries of concern would be permitted so long as they comply with the cybersecurity program, reporting, and recordkeeping requirements outlined below.

Exemptions

The rule creates a number of exemptions from the restrictions and prohibitions described above, including for:

– **U.S. Government activity**. Data transactions conducted pursuant to a contract, grant, or other agreement with federal departments and agencies, even when there is concurrent funding from non-federal sources, are exempt.

– **Personal communications** that do not involve the transfer of anything of value.

– **Information and informational materials with an expressive purpose** that are imported or exported to/from any country and metadata related to such materials. This is meant to be consistent with the Berman Amendment of the International Emergency Economic Powers Act (IEEPA).

Copyright 2025 Davis Polk & Wardwell LLP

- **Financial services**. Data transactions to the extent they are ordinarily incident to and part of the provision of financial services involving covered persons or countries of concern are exempt. Financial services include classic banking activities but also extend to the transfer of personal financial data or covered personal identifiers incidental to the purchase and sale of goods and services and the provision of investment management services. The exemption does not apply where it is not ordinarily incident to and necessary for the transaction, such as offshoring to a country of concern data processing for financial transactions not involving covered persons or providing bank directors or employees who are covered persons access to bulk personal data not necessary for processing exempt transactions. Sharing financial data as part of routine regulatory reporting, or for industry-standard fraud identification, AML/CFT, or sanctions compliance purposes, is covered by this exemption.
- **Corporate group transactions**. Intra-entity transactions between a U.S. person and its covered subsidiary or affiliate that are ordinarily incident to administrative or ancillary business operations (such as HR data), but not, for example, for R&D activities or support of U.S. customers. The boundaries of the exemption are somewhat unclear, and DOJ has indicated that public guidance on the scope this exemption is forthcoming.
- **CFIUS.** Investment agreements with respect to which CFIUS has exercised its jurisdiction to enter into or impose mitigation measures relating to data security that specifically supersede those in the rule.[5]
- **Telecom.** Data transactions, other than those involving data brokerage, are exempt to the extent that they are ordinarily incident to and part of the provision of voice and data communications services regardless of format or mode of delivery, including communications services delivered over cable, Internet Protocol, wireless, fiber, or other transmission mechanisms, as well as arrangements for network interconnection, transport, messaging, routing, or international voice, text, and data roaming.
- **Medical product authorizations**. Sensitive personal data that is re-identified or pseudonymized consistent with FDA guidelines required to be submitted to a country of concern regulatory entity to obtain or maintain authorization or approval to research or market a drug, biological product, device, or combination product and is reasonably necessary to assess the safety and effectiveness of such product is exempt.
- **Clinical investigations**. Data transactions ordinarily incident to a Food and Drug Administration (FDA) investigation or an FDA application are exempt. Transactions involving de-identified post-marketing safety and surveillance data necessary to support or maintain an FDA authorization are also exempt.

What does compliance entail?

Knowledge standard

The rule's restrictions and prohibitions apply to circumstances where a U.S. person **has actual knowledge or reasonably should have known** the transaction involved access to bulk sensitive personal data or U.S. government data by a covered person. The DOJ declined to specify a level of diligence that, if resulting in no red flags, would indicate a person did not have reason to know a transaction involved access to covered data, though it indicated it may do so at a later date. In general, the DOJ has signaled that it intends to use the constructive knowledge element of the rule as an important tool in combatting willful blindness and reckless behavior. Ignoring or taking an overly optimistic view of ambiguous but potential suspicious diligence findings is unlikely to be a wise compliance strategy.

Cybersecurity compliance program requirements for restricted transactions

The rule requires persons engaged in restricted transactions to adopt a written data compliance program, overseen and certified by an officer, director, or other employee responsible for data compliance. The program must comply with substantive requirements issued in parallel by CISA, which in turn incorporate existing federal standards such as those promulgated by the National Institute of Standards and Technology (NIST). The January 2025 CISA requirements are attached as Appendix B, but at a high level they require a U.S. company engaged in restricted transactions to adopt a written plan incorporating organizational measures, systems measures, and data-level measures:

- **Organizational measures** include designating an employee responsible for data security; maintaining updated inventories of IT assets to the extent practicable and a topology of relevant networks; implementing approval processes before the connection of new hardware, firmware or software; and responding to incidents and vulnerabilities within specified timeframes.

Copyright 2025 Davis Polk & Wardwell LLP

- **Systems measures** generally relate to maintaining logical and physical access controls to prevent access to covered data by covered persons or countries of concern. These include implementation of multifactor authentication, maintenance of systems logs related to access and security events, and maintenance of procedures for secure provisioning and timely revocation of access credentials.
- **Data-level measures** include data retention and deletion policies to minimize data at risk; aggregation, pseudonymization, de-identification or anonymization of data; encryption techniques; and privacy enhancing technologies, such as privacy preserving computation (e.g., homomorphic encryption), or differential privacy techniques (e.g., injecting sufficient noise into processing of data to preclude the reconstruction of covered data from the processed data).

In addition to these measures, the program must provide for:

- **Required due diligence procedures** for restricted transactions include risk-based procedures for verifying data flows, including the types and volumes of data involved in the transactions, the identity of the transaction parties (including ownership and citizenship or residence), the end use of the data, and the method of data transfer.
- **Annual audits** are required for U.S. persons engaging in restricted transactions, covering compliance with the data security and other requirements applicable to restricted transactions for every year the person engages in restricted transactions. In a change from the NPRM, the audit may be internal rather than external, if the internal audit meets standards of independence to be published in future guidance.
- **Record retention** for 10 years is required for full records of each restricted transaction, due diligence conducted, and the results of each audit.

The due diligence and audit requirements are not effective until October 6, 2025.

Reporting requirements

The rule would also impose various reporting requirements:

- Persons engaged in restricted data transactions must provide reports to the DOJ upon request.
- U.S. persons that have 25% or more of their equity interests owned, directly or indirectly, by a country of concern or covered person and that are engaged in a restricted transaction involving cloud-computing services must submit annual reports on such transaction(s).
- U.S. persons that have received and affirmatively rejected (including automatically) an offer from another person to engage in a prohibited transaction involving data brokerage must report the transaction to the DOJ within 14 days.
- U.S. persons engaged in data brokerage transactions with foreign persons that are not covered persons must report any known or suspected breaches of the required contractual prohibition on on-selling data to covered persons or countries of concern within 14 days of becoming aware of such a breach.

Licensing and interpretive guidance

The rule provides for obtaining both licenses for otherwise impermissible transactions and advisory opinions on the scope of the rule from DOJ. DOJ may issue general licenses, which are publicly available and authorize otherwise impermissible transactions without further action by the person relying on the license, subject to the terms and conditions of the license. Parties may also apply for a specific license to authorize an otherwise impermissible transaction, including information such as the parties, the types and volumes of data involved, the end use of the data, and the method of transfer. DOJ provides a non-binding target of 45 days for responding to a license application once it is complete and all requested information has been provided. Parties may also request an advisory opinion with respect to the application of the rule to a specific planned future transaction; the transaction must be real rather than hypothetical, and the application must provide all relevant details and cannot be anonymous. DOJ's target for responses to advisory opinion requests is 30 days.

Penalties

Noncompliance with the rule, material misstatements or omissions in connection with reporting and other requirements of the rule, false certifications or submissions, or other violations would be subject to a civil penalty not to exceed the greater of $368,136 per violation or an amount that is twice the amount of the transaction that is the basis of the violation. Willful violations can result in criminal penalties, such as a fine of up to $1 million or imprisonment of up to 20 years.

Copyright 2025 Davis Polk & Wardwell LLP

Preparing for compliance

The new rule will have wide-ranging impacts on U.S. businesses, particularly for firms that regularly engage in or with persons of countries of concern through commercial arrangements or seek investment from the same. The breadth of the rule means that new data security standards will apply to a wide range of commercial transactions, involving businesses with varied sizes and sophistication—creating the potential for widespread implementation challenges. Even sophisticated players will have to determine how their existing practices map to the new data security requirements and newly monitor whether their transactions implicate the rule. And these impacts will be felt soon, with U.S. persons expected to comply with the core requirements of the rule by April 8, 2025.

Notwithstanding additional clarifications made by DOJ in issuing the final rule, many gray areas remain to be resolved. Both DOJ and CISA have indicated intent to use their licensing and interpretive powers to address problems of fit as regulated entities begin to adapt to the rule. However, such guidance will remain under development during the initial implementation period.

In the absence of more specific guidance from the relevant agencies, companies can prepare by:

- Completing an inventory of their existing data to determine whether they maintain Covered Data.
- Mapping existing data security procedures to the CISA standards. The results can be used to determine any gaps and begin implementation.
- To the extent potentially restricted or prohibited by the rule, updating any transaction documents signed prior to the effective date but expected to close after to avoid disruption.
- Consider preparing to submit an application for a specific license if faced with a large number of potentially prohibited transactions.

While companies' commercial activities will be covered by the rule beginning in April 2025, the rule's affirmative due diligence, reporting, and auditing requirements will not take effect until 270 days after publication in the Federal Register. U.S. businesses that maintain Covered Data should begin putting in place policies and processes that will enable compliance with these requirements later this year.

Copyright 2025 Davis Polk & Wardwell LLP

Appendix A: Sensitive personal data categories & bulk thresholds

Copyright 2025 Davis Polk & Wardwell LLP

Sensitive personal data sub-types and bulk thresholds		
Data type	**Definition(s)**	**Bulk threshold**[6]
Human 'omic data	Human genomic data is data representing the nucleic acid sequences that constitute the entire set or a subset of the genetic instructions found in a human cell, including the result or results of an individual's "genetic test" (as defined in 42 U.S.C. 300gg-91(d)(17)) and any related human genetic sequencing data.	>1,000 U.S. persons generally; >100 persons for huma genomic data
Biometric identifiers	Measurable physical characteristics or behaviors used to recognize or verify the identity of an individual, including facial images, voice prints and patterns, retina and iris scans, palm prints and fingerprints, gait, and keyboard usage patterns that are enrolled in a biometric system and the templates created by the system.	>1,000 U.S. persons
Precise geolocation data	Data, whether real-time or historical, that identifies the physical location of an individual or a device with a precision of within 1,000 meters.	>1,000 U.S. persons or devices
Personal health data	Health information that indicates, reveals, or describes the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual. This term includes basic physical measurements and health attributes (such as bodily functions, height and weight, vital signs, symptoms, and allergies); social, psychological, behavioral, and medical diagnostic, intervention, and treatment history; test results; logs of exercise habits; immunization data; data on reproductive and sexual health; and data on the use or purchase of prescribed medications.	>10,000 U.S. persons
Personal financial data	Data about an individual's credit, charge, or debit card, or bank account, including purchases and payment history; data in a bank, credit, or other financial statement, including assets, liabilities, debts, or trades in a securities portfolio; or data in a credit report or in a "consumer report" (as defined in 15 U.S.C. 1681a(d)).	>10,000 U.S. persons

Copyright 2025 Davis Polk & Wardwell LLP

Covered personal identifiers	Any listed identifier[7]: (1) In combination with any other listed identifier; or (2) In combination with other data that is 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. The term covered personal identifiers excludes: (1) Demographic or contact data that is linked only to other demographic or contact data; and (2) A network-based identifier, account-authentication data, or call-detail data that is linked only to other network-based identifier, account-authentication data, or call-detail data as necessary for the provision of telecommunications, networking, or similar service.	>100,000 U.S. persons

Copyright 2025 Davis Polk & Wardwell LLP

Appendix B: CISA Security Requirements for Restricted Transactions

The following proposed security requirements can be found in their original form on the CISA website at https://www.cisa.gov/resources-tools/resources/proposed-security-requirements-restricted-transactions*. We have duplicated them below for your convenience. This appendix is not an official copy of those requirements and may reflect non-substantive differences in format.*

Security requirements for restricted transactions

Pursuant to Exec. Order 14117, *Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern*

On February 28, 2024, President Biden signed Executive Order (E.O.) 14117, Preventing Access to Americans' Bulk Sensitive Personal Data and U.S. Government-Related Data by Countries of Concern, to address national-security and foreign-policy threats that arise when countries of concern and covered persons can access bulk U.S. sensitive personal data or government-related data that may be implicated by the categories of restricted transactions.

As directed by E.O. 14117, CISA has developed the following security requirements to apply to classes of restricted transactions identified in regulations issued by the Department of Justice (DOJ). *See generally* 28 C.F.R. part 202 (identifying classes of restricted transactions at 28 C.F.R. § 202.401).

Background

The security requirements are designed to mitigate the risk of sharing U.S. government-related data or bulk U.S. sensitive personal data with countries of concern or covered persons through restricted transactions.[8] They do this by imposing conditions specifically on the covered data, as defined below, that may be accessed as part of a restricted transaction; on the covered systems, as defined below, more broadly; and on the organization as a whole. While the requirements on covered systems and on an organization's governance of those systems apply more broadly than to the data at issue and the restricted transaction itself, CISA assesses that implementation of these requirements is necessary to validate that the organization has the technical capability and sufficient governance structure to appropriately select, successfully implement, and continue to apply the covered data-level security requirements in a way that addresses the risks identified by DOJ for the restricted transactions. For example, to ensure and validate that a covered system denies covered persons access to covered data, it is necessary to maintain audit logs of such accesses as well as organizational processes to utilize those logs. Similarly, it is necessary for an organization to develop identity management processes and systems to establish an understanding of what persons may have access to different data sets.

In addition to requirements on covered systems, applying security requirements on the covered data itself that may be accessed in a restricted transaction is also necessary to address the risks. The specific requirements that are most technologically and logistically appropriate for different types of restricted transactions may vary. For example, some transactions may be amenable to approaches that minimize data or process it in such a way that does not reveal covered data to covered persons. In other cases, techniques such as access control and encryption may be more appropriate to deny any access by covered persons to covered data. The security requirements contemplate multiple options to minimize the risk to covered data, though all of the options build upon the foundation of the requirements imposed on covered systems and the organization as a whole. While U.S. persons engaging in restricted transactions must implement all of the organizational- and covered-system level requirements, such persons will have some flexibility in determining which combination of data-level requirements is sufficient to address the risks posed, based on the nature of the transaction, so long as the combination of security mechanisms deployed fully and effectively prevents access to covered data that is linkable, identifiable, unencrypted, or decryptable using commonly available technology by covered persons and/or countries of concern. If a combination of security mechanisms proves to be insufficient to prevent such access, that combination of security mechanisms will be considered invalid in protecting future access to covered data by covered persons.

In general

Copyright 2025 Davis Polk & Wardwell LLP

The security requirements provide the organizational- and covered system-level requirements (Section I) and covered data-level requirements (Section II) which U.S. persons engaging in restricted transactions must meet. These security requirements are in addition to any compliance-related conditions imposed in applicable DOJ regulations. *See* 28 C.F.R. § 202.1001—202.1201. References below to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF),[9] NIST Privacy Framework (PF),[10] and CISA's Cross-Sector Cybersecurity Performance Goals (CPGs)[11] are intended to help the reader understand which aspects of existing frameworks, guidance, or other resources these security requirements are based upon, consistent with the requirements of the E.O. Understanding and applying these security requirements does not require a reader to also understand and apply the referenced resources.

Definitions

To the extent these security requirements use a term already defined in DOJ's regulation, *see* 28 C.F.R. § 202.201-202.259, CISA's use of that term below carries the same meaning.

For the purpose of these security requirements:

- Asset means data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes.
- Covered data means government-related data bulk U.S. sensitive personal data.[12]
- Covered system:
- means an information system used to obtain, read, copy, decrypt, edit, divert, release, affect, alter the state of, view, receive, collect, process, maintain, use, share, disseminate, or dispose of (collectively, "interact with") covered data as part of a restricted transaction, regardless of whether the data is encrypted, anonymized, pseudonymized, or de-identified; and
- does not include an information system (e.g., an end user workstation) that has the ability to view or read sensitive personal data (other than sensitive personal data that constitutes government-related data) but does not ordinarily interact with such data in bulk form.[13]
- Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
- Network means a system of interconnected components, which may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

Security requirements

I. *Organizational- and System-Level Requirements.* For any covered system:
   a. Ensure basic organizational cybersecurity policies, practices, and requirements, including all of the following, are in place:
      i. Identify, prioritize, document all assets of the covered system.
         A. Maintain, to the maximum extent practicable, an updated inventory of covered system assets with each system's respective internet protocol (IP) address (including IPv6).[14] (*NIST CSF 2.0 ID.AM-01, CISA CPGs 1.A*)
         B. Ensure inventory is updated on a recurring basis, no less than monthly for Information Technology (IT) assets. (*NIST CSF 2.0 ID.AM-08, CISA CPGs 1.A*)
      ii. Designate, at an organizational level, an individual (e.g., a Chief Information Security Officer) responsible and accountable for (1) cybersecurity and (2) governance, risk, and compliance functions (GRC). This could be one individual responsible and accountable for both areas, or one individual for each of these two areas. (*NIST CSF 2.0 GV.RR-02, CISA CPGs 1.B*)
      iii. Remediate known exploited vulnerabilities (KEVs) in internet-facing systems within a risk-informed span of time, prioritizing the most critical assets first and completing remediation for all such vulnerabilities within 45 calendar days. (*NIST CSF 2.0 ID.RA-01 and 08 CISA CPGs 1.E*)
         A. Implement alternative compensating requirements, should patching not be feasible.
         B. Establish a process to evaluate, after patching, whether internet-facing covered systems with KEVs were compromised prior to patching.
      iv. Document and maintain all vendor/supplier agreements for covered systems (e.g., third-party network connection agreements), including contractual IT and cybersecurity requirements. (*NIST CSF 2.0 GV.SC-05, 06, 07, 10, CISA CPGs 1.G, 1.H, 1.I*)

Copyright 2025 Davis Polk & Wardwell LLP

v. Develop and maintain an accurate network topology of the covered system and, to the extent technically feasible, any network interfacing with a covered system to facilitate visibility into connections between assets, and aid in timely identification of and response to incidents. (*NIST CSF 2.0 ID.AM-03, CISA CPGs 2.P*)
vi. Adopt and implement an administrative policy that requires approval before new hardware or software is deployed in/on a covered system. U.S. persons engaging in restricted transactions must maintain a risk-informed allowlist of approved hardware and software for covered systems. (*NIST CSF 2.0 GV.PO-02, ID.RA-09, ID.AM-08, PR.PS-01, 02, 03, CISA CPGs 2.Q*)
vii. Develop and maintain incident response plan(s) applicable to covered systems, which should be reviewed annually and updated as appropriate. (*NIST CSF 2.0 ID.IM-04, CISA CPGs 2.S, 5.A*)

b. Implement logical and physical access controls to prevent covered persons or countries of concern from gaining access to covered data that that does not comply with the data-level requirements (Section II) including through information systems, cloud-computing platforms, networks, security systems, equipment, or software. (*NIST CSF 2.0 PR.AA-01 through PR.AA-06*) Specifically, U.S. persons engaging in restricted transactions must:
i. Enforce multifactor authentication (MFA) on all covered systems (e.g., by requiring an Authentication Assurance Level (AAL) AAL2 or AAL3 authenticator as defined in the most recent version of NIST Special Publication 800-63B and/or its supplements), or in instances where MFA is not technically feasible and/or not enforced, require passwords have sufficient strength, including sufficient length of 15 or more characters. (*NIST CSF 2.0 PR.AA-03, PR.AA-04, CISA CPGs 2.B, 2.H*)
ii. Promptly revoke (e.g., on day of departure or within a risk-informed timeframe) any individual credentials, shared credentials, and/or authorized access to covered systems upon termination or change in roles for any individual with access to covered system(s). (*NIST CSF 2.0 GV.RR-04, PR.AA-01, & PR.AA-04, CISA CPGs 2.D*)
iii. Collect logs for covered systems pertaining to access- and security-focused events (e.g., intrusion detection systems/intrusion prevention systems, firewall, data loss prevention, virtual private network, and detection of unsuccessful login events), and store such logs for use in both detection and incident response activities (e.g., forensics to assist in detection, response, and recovery). Implement a process to notify cybersecurity personnel when a critical log source, such as an operating system event logging tool, is not producing and retaining logs as expected. (*NIST CSF 2.0 PR.PS-04, & DE.CM-03, and 09, CISA CPGs 2.T, 2.U*)
A. Securely store collected logs in a central system, such as a security information and event management tool or central database, for at a minimum 12 months. In the event of a data breach or a violation of these security requirements, logs should be maintained until final resolution of the matter by the U.S. Government.
B. Ensure that collected logs may only be accessed or modified by authorized and authenticated users.
iv. Implement configurations to deny by default (e.g., by requiring authentication) all connections to covered systems and any network on which covered systems reside, unless connections are explicitly allowed for specific system functionality. (*NIST CSF 2.0 PR.PS-01*)
v. Issue and manage, at an organizational level, identities and credentials for authorized users, services, and hardware, with sufficient attributes available to prevent access by covered persons or countries of concern to covered data that that does not comply with the data-level requirements (Section II). Limit system access to the types of transactions and functions that authorized users are permitted to execute. (*NIST CSF 2.0 PR.AA-05, CISA CPGs 2.C*)

c. Conduct an internal data risk assessment that evaluates whether and how the overall approach selected and implemented pursuant to Section II sufficiently prevents access to covered data that is linkable, identifiable, unencrypted, or decryptable using commonly available technology by covered persons and/or countries of concern, taking into consideration the likelihood of disclosure and the likelihood of harm based on the nature of the transaction and the data at issue, to include potential data misuse and associated consequences. The risk assessment must include a mitigation strategy outlining how implementation will prevent access to covered data that is linkable, identifiable, unencrypted, or decryptable using commonly available technology by covered persons and/or countries of concern. The risk assessment should be reviewed annually by the organization and updated as appropriate. (*NIST Privacy Framework ID.RA-P1, NIST Privacy Framework ID.RA-P3, NIST Privacy Framework ID.RA-P4, NIST Privacy Framework ID.RA-P5)*

II. *Data-Level Requirements.* For any restricted transaction, implement a combination of the following mitigations that, taken together, is sufficient to fully and effectively prevent access to covered data that is linkable, identifiable, unencrypted, or decryptable using commonly available technology by covered persons and/or countries of concern, consistent with the data risk assessment described in Section I.C.:

a. Apply data minimization and data masking strategies to reduce the need to collect, or sufficiently obfuscate, respectively, covered data to prevent visibility into that data, without precluding the U.S. persons engaging in restricted transactions from conducting operations with the data. These strategies must include:
i. Maintaining and implementing a written data retention and deletion policy, to be reviewed annually and updated as appropriate. (*NIST Privacy Framework GV.PO-P1, CT.PO-P2*)
ii. Processing data in such a way to either render it no longer covered data or minimize the linkability to U.S. person entities before it is subject to access by a covered person or country of concern. (*NIST Privacy Framework CT.DP-P2*)

Copyright 2025 Davis Polk & Wardwell LLP

A. This may be achieved through application of techniques such as aggregation, pseudonymization, de-identification, or anonymization.
B. When implemented, observability and linkability of data must be minimized to ensure U.S. person identities cannot be inferred or extrapolated from the individual data set at issue or in combination with other data sets the recipient or recipient-linked organizations are known to hold.
C. Aggregations of covered data must be based on at least the number of records required to render the data "bulk" under the regulations found at 28 C.F.R. § 202.205.

iii. Treating information systems that implement such processing as covered systems subject to the requirements of Section I. (*NIST Privacy Framework CT.DP-P4, CM.AW-P3, GV.PO-P2*)

b. Apply encryption techniques to protect covered data during the course of restricted transactions. These techniques must include:
   i. Comprehensive Encryption: Encrypt covered data in a restricted transaction, regardless of type, during transit and storage.[15] (*NIST Privacy Framework CT.DP-P1, PR.DS-P1, PR.DS-P2, CISA CPGs 2.K*)
   ii. Key Management: Generate and securely manage cryptographic keys used to encrypt covered data, including the following practices: (*NIST Privacy Framework CT.DP-P1 & PR.DS-P2, CISA CPGs 2.L*)
      A. Do not co-locate encryption keys with covered data.
      B. Do not store encryption keys, via any mechanism (physically or virtually), in a country of concern.
      C. Covered persons must not be authorized to have access to encryption keys.
      D. All information systems responsible for the storage of and access to encryption keys must be considered covered systems subject to the requirements of Section I.
c. Apply privacy enhancing technologies, such as privacy preserving computation (*e.g.*, homomorphic encryption), or differential privacy techniques (*e.g.*, inject sufficient noise into processing of data to preclude the reconstruction of covered data from the processed data), to process covered data. Use of such techniques are subject to the following:
   i. The application of privacy enhancing technologies must not reveal to covered persons participating in the restricted transaction covered data or information that could reasonably likely be used to reconstruct covered data, including by linking processed data with other data sets (*e.g.*, allowing a covered person to participate in a privacy preserving computation that requires trusted parties would not be permissible).
   ii. For the avoidance of doubt, information systems that implement such processing are covered systems subject to the requirements of Section I. (*NIST Privacy Framework CT.DP-P1*)
d. Configure the previously outlined identity and access management techniques to deny authorized access to covered data by covered persons and countries of concern within all covered systems. (*NIST Privacy Framework PR.AC-P4*)

Copyright 2025 Davis Polk & Wardwell LLP

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Robert A. Cohen
+1 202 962 7047
robert.cohen@davispolk.com

James W. Haldin
+1 212 450 4059
james.haldin@davispolk.com

Paul Marquardt
+1 202 962 7156
paul.marquardt@davispolk.com

Martin Rogers
+852 2533 3307
martin.rogers@davispolk.com

Will Schisa
+1 202 962 7129
will.schisa@davispolk.com

Paul S. Scrivano
+1 650 752 2008
+1 212 450 4304
paul.scrivano@davispolk.com

Paul Shortell
+1 202 962 7158
paul.shortell@davispolk.com

Miranda So
+852 2533 3373
miranda.so@davispolk.com

Patrick Q. Sullivan
+1 202 962 7179
patrick.sullivan@davispolk.com

This communication, which we believe may be of interest to our clients and friends of the firm, is for general information only. It is not a full analysis of the matters presented and should not be relied upon as legal advice. This may be considered attorney advertising in some jurisdictions. Please refer to the firm's privacy notice for further details.

1 The rule defines linkable as "reasonably capable of being linked." Linked means associated. This implies that U.S. persons may need to make probabilistic judgments about whether a hostile actor could link data. Practically, if a company employs a covered person the employee is likely to have access to a variety of information that could make data linkable.

2 Demographic identifiers linked solely to other demographic identifiers (e.g., a list of names and addresses) are also not sensitive personal data.

3 The combination of encrypted data with other encrypted or unencrypted data is treated the same as the combination of two unencrypted datasets for the purposes of determining whether linked data is sensitive personal data.

4 The rule defines a "former senior official" as either a "former senior employee" or "former very senior employee," as those terms are defined in the ethics regulations pertaining to post-employment conflicts of interest for former Executive Branch or independent agency employees.

5 Aa practical matter, in most cases parties to an investment will not know whether CFIUS will exercise that authority until shortly before closing the transaction and so must plan to meet the cybersecurity requirements if relevant.

6 In cases where data is combined the lowest threshold applicable to an involved data type would be used.

Copyright 2025 Davis Polk & Wardwell LLP

[7] A listed identifier means a full or truncated government identification or account number, full financial account numbers or personal identification numbers associated with a financial institution or financial-services company, device-based or hardware-based identifier, demographic contact data, advertising identifier, account authentication data, network-based identifier, or call-detail data.

[8] CISA notes that these security requirements are, as required by the E.O., designed to "address the unacceptable risk posed by restricted transactions, as identified by the Attorney General." E.O. 14117 Sec. 2(d). They are not intended to reflect a comprehensive cybersecurity program. For example, several areas addressed in CISA's Cross-Sector Cybersecurity Performance Goals (CPGs), available at https://www.cisa.gov/cross-sector-cybersecurity-performance-goals, are not reflected in the data security requirements, even though the CPGs themselves are a common set of protections that CISA recommends all critical infrastructure entities voluntarily implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques. As the operational lead for federal cybersecurity and national coordinator for critical infrastructure security and resilience, CISA recommends that all U.S. persons implement cybersecurity best practices in light of the risk and potential consequence of cyber incidents.

[9] NIST, Cybersecurity Framework ver. 2.0, available at https://www.nist.gov/cyberframework.

[10] NIST, Privacy Framework ver. 1.0, available at https://www.nist.gov/privacy-framework.

[11] CISA, Cross-Sector Cybersecurity Performance Goals, available at https://www.cisa.gov/cross-sector-cybersecurity-performance-goals.

[12] ***Contextual note:*** *There appears to be a missing "or" in the published version. We have reproduced the published version as-is and thus have not corrected it.*

[13] For example, if an end user workstation only interacts with individual records of U.S. sensitive personal data, although it may have the ability to "read" or "view" bulk U.S. sensitive personal data, it is not deemed on its own to be a covered system unless it takes further actions outlined in the definition of covered system (e.g., maintaining or processing data in excess of the bulk thresholds) with respect to such data. Note that there are no bulk thresholds for government-related data and individual records would be considered covered data. Thus, end user workstations that interact with government related data are covered systems.

[14] This list may be maintained in an automated fashion that tracks dynamic changes in the covered system (e.g., automatic provisioning of virtual machines or containers in a cloud environment) and may consist of several constituent parts for discrete subsystems.

[15] For the purposes of this requirement, CISA considers comprehensive encryption to mean cryptographic algorithms, ciphers, and protocols that are ordinarily accepted by U.S. persons with significant expertise in cryptography as being sufficient to provide confidentiality and integrity protections to sensitive data against compromise by currently known techniques and a level of computing power that is reasonably foreseeable to be available to any person, organization, or country in the near future. CISA considers U.S. Government approved encryption algorithms, ciphers, and protocols to meet this standard, but organizations may determine that other algorithms, ciphers, and protocols also qualify. For connections made using Transport Layer Security (TLS), only version 1.2 or higher is considered comprehensive encryption.

Copyright 2025 Davis Polk & Wardwell LLP