Davis Polk

DOJ issues proposed rule restricting sensitive data transfers to China and other adversary countries

November 22, 2024 | Client Update

The proposed rule would limit U.S. persons from providing access to "bulk" U.S. sensitive personal data and government-related data to persons located in or connected to countries perceived as hostile. Many U.S. businesses have such data and would be required to impose data security standards before engaging in investment, employment or vendor agreements with covered persons. Many outright sales of data or commercial agreements involving access to human genomic data would be prohibited.

On October 21, 2024, the Department of Justice (DOJ) issued a notice of proposed rulemaking (Proposed Rule) that, if adopted, would impose data security requirements on or prohibit certain covered data transactions by U.S. persons with foreign persons connected to **countries of concern**, which the Proposed Rule defines to include China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia and Venezuela. The Proposed Rule is issued pursuant to Executive Order 14117, "Preventing Access to Americans' Bulk Sensitive Data and United States Government-Related Data by Countries of Concern" and follows an advanced notice of proposed rulemaking (ANPRM) issued concurrently with Executive Order 14117 in February 2024. The Proposed Rule generally follows the framework laid out in the DOJ's February 2024 ANPRM, discussed in our previous client update, with some notable changes discussed below.

In conjunction with the Proposed Rule, the Cybersecurity & Infrastructure Security Agency (CISA) has issued a separate request for comment on proposed data security requirements that are incorporated by reference into the Proposed Rule. These are attached as Appendix B.

Comments to both the DOJ and CISA are due by November 29, 2024. Based on public statements from the DOJ staff, DOJ intends to move as quickly as possible and is targeting issuing a final rule in early 2025; the change in administration could in principle introduce some delay, but access to data on U.S. persons by potential foreign adversaries has been a long-standing national security concern across the past several administrations, both Republican and Democratic.

What does the Proposed Rule do?

The Proposed Rule would prohibit U.S. persons and companies from engaging in **data brokerage** transactions with **covered persons** located in or owned by residents of **countries of concern** (China, Russia, Cuba, Iran, North Korea and Venezuela) involving broad categories of **bulk U.S. sensitive personal data** or **government-related data** (Restricted Data). It would also prohibit U.S. companies holding any significant quantity of **human genomic data** from accepting investments (other than small passive

investments in publicly traded securities) from covered persons or engaging covered persons in employee or vendor relationships with access to such data.

More significantly, it would also require U.S. persons and companies to meet fairly extensive government-mandated cybersecurity requirements before engaging in a range of ordinary commercial transactions with covered persons. These requirements include meeting cybersecurity standards set by the CISA, adopting formal written cybersecurity policies overseen by a responsible security officer, and conducting cybersecurity audits at least annually, as well as due diligence and recordkeeping requirements. The relevant transactions include any **employment agreement** or **vendor agreement** in which a covered person will have access to Restricted Data, including access via the cloud. They also include any **investment agreement** involving an investment by a person of a country of concern holding any Restricted Data – whether or not the investor will have any access at all to such data – 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.

Effectively, U.S. businesses holding Restricted Data will have to adopt cybersecurity plans meeting the standards set out in the Proposed Rule or be barred from using Chinese (and other) employees or vendors to work with Restricted Data or accepting any significant investment from covered persons. With respect to individuals, the rule is based on the location rather than the citizenship of the person (except that U.S. citizens are exempt, even if located in a country of concern); with respect to entities, it is based on organization, location, or control by a country of concern.

Practically speaking, this means that **any time** a U.S. company holding bulk sensitive U.S. data or government-related data transfers such data to, or enters into an employment, vendor, or investment relationship with, a person or company located in or organized under the laws of China, Cuba, Iran, North Korea, Russia or Venezuela, or a subsidiary, employee or contractor of such a company, it should consider whether the proposed restrictions apply. The Proposed Rule has no pre-clearance or review process; it is an enforcement-based regime. U.S. persons therefore bear the burden of doing sufficient diligence (both on the data they themselves hold and on their potential counterparties) to determine whether the Proposed Rule's restrictions apply.

Mechanics of the Proposed Rule

Foreign persons targeted

The Proposed Rule only applies to transactions that could provide access to sensitive data to **covered persons**, which are generally defined as any foreign person that is:

- an entity that is 50% or more owned, directly or indirectly, 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 covered person;
- a foreign individual who is primarily a resident in the territorial jurisdiction of a country of concern; or
- an entity that is 50% or more owned, directly or indirectly, by any of the foregoing or a designated covered person.

U.S. citizens, U.S. nationals, lawful permanent residents, lawful refugees and asylum grantees, entities organized solely under U.S. law (including foreign branches), and foreign persons or entities physically within the United States are not covered persons. In addition to persons meeting the general rules above, covered persons may be designated by the Attorney General under the Proposed Rule (for example, because they are acting on behalf of covered persons).

Persons required to comply

Only U.S. persons are required to comply with the Proposed Rule. While transactions among non-U.S. persons are therefore generally not covered, the Proposed Rule has certain collateral consequences for transactions even solely among non-U.S. persons:

- U.S. persons may not knowingly direct a foreign person to engage in a transaction that would be a prohibited transaction if the foreign person were a U.S. person. Only persons with authority to make decisions for or on behalf of an entity can direct an entity. Thus, a U.S. person who is an officer or senior manager of a foreign person that engages in a data brokerage transaction with a covered person would violate the Proposed Rule but an employee that processes the payment for the transaction would likely not be in violation.
- If a U.S. person engages in a data brokerage transaction with a foreign person that it knows or should have known is a front for a covered person, the U.S. person will be in violation of the Proposed Rule.
- U.S. persons are also required to impose contractual obligations in data brokerage transactions involving foreign persons that are not covered persons prohibiting the on-selling of data to covered persons.

Restricted data

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

Bulk U.S. sensitive personal data

The Proposed Rule defines "**sensitive personal data**" to include **precise geolocation data**, **biometric identifiers**, **human genomic 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 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.

Stand-alone lists of personal identifiers 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, 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]

Importantly, for purposes of the Proposed Rule's coverage, it does not matter whether the data is anonymized or encrypted. Compliance with CISA's standards for anonymization and encryption can make a transaction that would otherwise be prohibited permissible, but the use of encryption does not itself remove data from the scope of the Proposed Rule.

The Proposed Rule would only apply restrictions to transactions over a specified "bulk" threshold, which is determined based on the total volume of data transacted over the preceding 12 months. The threshold varies widely depending on the type of data involved. The relevant data volumes and types are set forth on Appendix A.

U.S. government-related data

Government-related data comprises two categories of data:

- **Precise geolocation data** for any location that is within one of the eight areas listed on the Government-Related Location Data List included in the Proposed Rule. Additional areas may be added by the Attorney General.

[1] The Proposed Rule defines linkable as "reasonably capable of being linked." 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.

- **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 Proposed Rule's restrictions are targeted at transactions, not the collection or use of covered types of data by U.S. persons. However, the categories of transactions covered by the Proposed Rule are defined broadly and cover a number of situations beyond simply selling data to a country of concern or covered person.[5] These include:

- **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 covered by the data. In response to comments on the ANPRM, DOJ clarified that "data brokerage" may include not only stand-alone sales of data, but sales or licensing of data (e.g., customer lists) in connection with bona fide commercial transactions.
- **Vendor agreement**: Any arrangement, other than an employment agreement, for providing goods or services to another person for consideration, including cloud computing services.
- **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.
- **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.
  - 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 which fall into the following three categories are not covered transactions:
    - investments made in publicly traded securities;
    - investments made in SEC-registered index funds, mutual funds or ETFs;
    - investments made as a limited partner in a pooled investment fund so long as certain criteria that would indicate the limited partner has influence over the fund's operations are not met.

    All three conditions (passivity, publicly traded security or investment through a fund, and less than 10% by vote and value) must be met, so that an investment by a U.S. private equity fund in which a covered person held a completely passive 11% interest would be a covered transaction.
  - The Proposed Rule clarifies by way of examples that any investment agreement not meeting the passive investment exclusion in a company that has access to bulk U.S. sensitive personal data or government-related data would be a covered data transaction even if the investment is noncontrolling and the foreign investor lacks any formal rights of access to data. (It is not entirely clear how this statement interacts with the "covered data transaction" definition above, which requires some access to Restricted Data; however, the Proposed Rule seems to imply that the mere possibility of influence is sufficient and does not mention any showing of actual access.)

Prohibitions and restrictions

Prohibited transactions

The Proposed 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,

[4] The Proposed 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] The Proposed Rule clarifies that a covered data transaction must involve *access* to covered data. However, "access" and "transaction" both remain broadly defined in the DOJ's proposal. Under the Proposed Rule, the term *access* means logical or physical access, including the ability to obtain, read, copy, decrypt, edit, divert, release, affect, alter the state of, or otherwise view or receive, in any form, including through information systems, information technology systems, cloud-computing platforms, networks, security systems, equipment, or software. Transaction is defined as any acquisition, holding, use, transfer, transportation exportation of, or dealing in data in which a foreign country or national (from any jurisdiction) has an interest.

covered data transactions with covered persons or countries of concern involving **data brokerage** or involving the **bulk transfer of human genomic 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 Proposed Rule would create a number of exemptions from the restrictions and prohibitions described above, including for:

- **Personal communications** that do not involve the transfer of anything of value.
- **Information and informational materials** that are imported or exported to/from any country.
- **Financial services.** Data transactions to the extent they are ordinarily incident to and part of the provision of financial services. 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.
- **Corporate group transactions.** Intra-entity transactions between a U.S. person and its subsidiary or affiliate that is a covered person that are ordinarily incident to ancillary business operations (such as HR data).
- **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 Proposed Rule.[6]
- **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 telecommunications services, including international calling, mobile voice, and data roaming**.**
- **Medical product authorizations.** De-identified sensitive personal data that is 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) investigations or an FDA application are exempt. Transactions involving de-identified post-marketing safety and surveillance data necessary to support or maintain authorization an FDA authorization are also exempt.

What does compliance entail?

Knowledge standard

The Proposed Rule would only 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 level of inquiry a person should make into the circumstances of a transaction is not precisely defined, with the Proposed Rule referring repeatedly to conducting “reasonable” due diligence on data, counterparties, and counterparties’ compliance with any contractual restrictions to identify restricted transactions.

[6] 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.

Davis Polk

Cybersecurity compliance program requirements for restricted transactions

The Proposed 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 proposed 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 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.
- **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 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** by an independent auditor 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.
- **Record retention** for 10 years is required for full records of each restricted transaction, due diligence conducted, and the results of each audit.

Reporting requirements

The Proposed 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 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.

Davis Polk

Penalties

Noncompliance with the Proposed Rule, material misstatements or omissions in connection with reporting and other requirements of the Proposed 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.

How will businesses be affected?

The DOJ staff has stated that it intends to move quickly and issue a final rule in early 2025. A final rule consistent with the Proposed Rule will have significant near-term impacts for both U.S. and foreign businesses, including foreign firms who are not covered persons.

Impacts for U.S. businesses

U.S. businesses that deal in data that could be considered sensitive personal data or government-related data will be affected in a number of ways.

- U.S. businesses that employ covered persons, engage with covered person vendors or receive investment from covered persons will need to track the full inventory and volume of data they hold, collect, or use to determine whether their activities are subject to the rule. This may entail monitoring previously untracked characteristics, such as the nationalities of the persons described by the data.
- U.S. businesses may need to conduct additional diligence on vendors and investors to understand whether they are covered persons. If a U.S. person engages in a data brokerage transaction with a foreign person that it knows or should have known is a front for a covered foreign person, the U.S. person will be in violation of the Proposed Rule.
- U.S. businesses potentially engaged in or intending to engage in restricted transactions will need to ensure that their policies and procedures comply with the cybersecurity program requirements outlined above, as well as audit and reporting requirements.
- U.S. companies selling or licensing bulk data to third parties, either as a stand-alone product or as part of a broader commercial offering, will likely need to suspend and wind down transactions with covered persons unless the DOJ issues a relevant general license or data brokers secure a specific license.
- U.S. businesses with parent companies or other affiliates in countries of concern may need to implement internal data transfer controls to ensure only transfers compliant with the corporate group exemption are made.

Impacts for foreign businesses and their U.S. personnel

While the Proposed Rule only imposes obligations on U.S. persons, there are likely to be collateral consequences for foreign firms that transact in bulk U.S. sensitive personal data or government-related data with covered persons or countries of concern. In particular, U.S. data brokers are required to impose contractual obligations in data brokerage transactions involving foreign persons that are not covered persons prohibiting the on-selling of data to covered persons. Thus, foreign but not covered person firms that are customers of U.S. data brokers may be contractually obligated to refrain from certain dealings with clients from countries of concern.

The Proposed Rule also prohibits U.S. persons from knowingly directing a foreign person to engage in a transaction that would be a prohibited transaction if the foreign person were a U.S. person. Persons with the authority to direct an entity are generally limited to officers, senior executives and persons of similar stature (not ordinary employees). Foreign businesses may need to develop compliance procedures to prevent U.S. person officers or directors from violating this prohibition.

Finally, although the Proposed Rule does not directly apply to non-U.S. persons, the underlying authorizing statute upon which the Proposed Rule relies (the International Emergency Economic Powers Act) prohibits

all persons from "conspiring to violate" or "causing a violation" of any regulation issued under the statute. It is possible that these provisions could be used to target foreign persons whose actions result in a U.S. person's violating the Proposed Rule, particularly in cases in which the foreign person deliberately deceived its U.S. counterparty or knowingly participated in a violation.

Impacts on investment

The Proposed Rule may lead to a significant decrease in investment by covered persons in U.S. companies in data-rich sectors. This will be particularly the case with respect to early-stage companies that may not have the resources or expertise to implement the required formal cybersecurity programs prior to closing.

The Proposed Rule could also affect investment by covered persons in pooled investment funds investing in the United States. While fund limited partners typically are already passive investors, for reasons including managing CFIUS risk, funds investing in the United States will need to ensure that no covered person has a greater than 10% indirect interest in the investment in order to avoid triggering the Proposed Rule.

More generally, U.S. companies seeking investment will likely conduct additional diligence on all foreign person investors. Likewise, covered person investors (who will indirectly bear the risk of noncompliance through potential imposition of financial penalties on U.S. businesses they acquire) may conduct additional diligence on data assets and security programs of U.S. targets.

Next steps

Comments on the Proposed Rule are due November 29, 2024. Given DOJ's ambition to issue a final rule quickly, U.S. companies should be prepared for the implementation of a final rule very similar to the Proposed Rule (though if the final rule is not issued before President Biden leaves office, it is possible that the Trump administration could delay or revise the rule). Potentially affected persons may find it prudent to take the following steps:

- Potentially affected persons should **review the data they collect or use**. The definitions of covered data in the Proposed Rule cover a wide variety of information. Even the workaday aggregation of otherwise innocuous data types, like covered personal identifiers, is effectively standard practice for many companies operating in e-commerce, marketing, business analytics and other data-intensive sectors. A company does not necessarily have to collect data itself. The examples in the Proposed Rule indicate that access can occur in other ways, such as when an analytics firm processes data on behalf of a customer.
- Companies or persons that deal in sensitive data should **consider their current and future exposure to covered person counterparties, vendors, employees or investors**. Most companies that engage in outright sales of data, i.e., data brokerage, will likely be well-positioned to understand their exposure to covered persons. However, other forms of covered data transactions are less noticeable and U.S. persons will need to be prepared to efficiently analyze HR data, investor details and vendor characteristics, among other things, to understand whether their ordinary course transactions could implicate a final rule. The final rule will not be retroactive, relieving U.S. persons of the obligation to examine current relationships, but analysis of current transactions will be a helpful guide to future situations that may implicate any final rule.
- **Data brokers** (i.e., any company that licenses or sells bulk sensitive data, including in connection with other products or services) and **persons that collect, use or store human genomic data** should be especially cognizant of any potential exposure to covered persons and be ready to curtail those relationships, seek a license or identify a relevant exemption.
- U.S. persons that deal in sensitive data and have potential exposure to covered persons **should determine whether relevant exemptions apply.** If not, such persons may wish to consider seeking a license upon the issuance of a final rule.
- U.S. persons that deal in sensitive data and have potential exposure to covered persons **should examine the cybersecurity program requirements** and determine the steps to bring existing data security measures in line.

Davis Polk

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

Robert A. Cohen	+1 202 962 7047	robert.cohen@davispolk.com
David I. Feinstein	+1 212 450 3293	david.feinstein@davispolk.com
James W. Haldin	+1 212 450 4059	james.haldin@davispolk.com
Daniel S. Kahn	+1 202 962 7140	daniel.kahn@davispolk.com
Paul D. Marquardt	+1 202 962 7156	paul.marquardt@davispolk.com
Paul J. Nathanson	+1 202 962 7055	paul.nathanson@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	paul.scrivano@davispolk.com
Paul Shortell	+1 202 962 7158	paul.shortell@davispolk.com

Davis Polk

Appendix A: Sensitive Personal Data Categories & Bulk Thresholds

Sensitive personal data sub-types and bulk thresholds		
Data type	**Definition**	**Bulk threshold[1]**
Human genomic data	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.	>100 U.S. persons
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 geolocations 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 relates to 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
Covered personal identifiers	Any listed identifier[2]: (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

[1] In cases where data is combined the lowest threshold applicable to an involved data type would be used.
[2] 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.

PROPOSED SECURITY REQUIREMENTS FOR RESTRICTED TRANSACTIONS

E.O. 14117 IMPLEMENTATION

PROPOSED 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 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 bulk U.S. sensitive personal data or U.S. government-related data with countries of concern or covered persons through restricted transactions.[1] They do this by imposing conditions specifically on the covered data, as defined below, that may be shared 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 are sufficient to address the risks posed, based on the nature of the transaction,

[1] 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 events.

so long as the combination of security mechanisms deployed fully and effectively prevents access to covered data by covered persons. If a combination of security mechanisms proves to be insufficient to prevent access to covered data by covered persons, those security mechanisms will be considered invalid in protecting future access to covered data by covered persons.

IN GENERAL

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),[2] NIST Privacy Framework (PF),[3] and CISA's Cross-Sector Cybersecurity Performance Goals (CPGs)[4] 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 EO. Understanding and applying these security requirements does not require a reader to also understand and apply the referenced resources.

DEFINITIONS

To the extent these proposed 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 bulk U.S. sensitive personal data or government-related data.*
- *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 covered data as part of a restricted transaction, regardless of whether the data is encrypted, anonymized, pseudonymized, or de-identified.*
- *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:

1. Identify, prioritize, document all assets of the covered system.

a. Maintain a regularly updated inventory of covered system assets with each system's respective internet protocol (IP) address (including IPv6). For hardware, this should also include MAC address. (*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*)

[2] NIST, Cybersecurity Framework ver. 2.0, available at https://www.nist.gov/cyberframework.
[3] NIST, Privacy Framework ver. 1.0, available at https://www.nist.gov/privacy-framework.
[4] CISA, Cross-Sector Cybersecurity Performance Goals, available at https://www.cisa.gov/cross-sector-cybersecurity-performance-goals.

2. 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)

3. Remediate known exploited vulnerabilities (KEVs) within 14 calendar days; other vulnerabilities (those not known to be exploited) must be remediated within 15 calendar days if deemed critical severity, or 30 calendar days if deemed high severity. (*NIST CSF 2.0 ID.RA-01 and 08 CISA CPGs 1.E*)

    a. Should patching not be feasible, alternative compensating requirements must be implemented.

    b. U.S. persons engaging in restricted transactions must document all mitigation measures (patch or compensating requirement) that are implemented.

4. 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*)

5. Develop and maintain an accurate network topology of the covered system and, to the maximum extent practicable, 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*)

6. Adopt and implement an administrative policy that includes a manual or automated process that requires approval before new hardware, firmware, or software/software version is installed or deployed in a covered system. (*NIST CSF 2.0 GV.PO-02, ID.RA-09, ID.AM-08, PR.PS-01, 02, 03, CISA CPGs 2.Q*)

    a. U.S. persons engaging in restricted transactions must maintain a risk-informed allowlist of approved hardware, firmware, and software for covered systems.

    b. The risk-informed allowlist must include specification of approved versions, for covered systems.

7. 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, in any form, 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:

1. Enforce multifactor authentication (MFA) on all covered systems, or in instances where MFA is not feasible, require passwords have sufficient strength, including sufficient length of 16 or more characters. (*NIST CSF 2.0 PR.AA-03, PR.AA-04, CISA CPGs 2.B, 2.H*)

2. Immediately revoke, upon termination or change in roles for any individual with authorized access to covered system(s), any credentials assigned to that individual. (*NIST CSF 2.0 GV.RR-04, PR.AA-01, & PR.AA-04, CISA CPGs 2.D*)

3. 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). Notify cybersecurity personnel when a critical log source, such as an operating system event logging tool, is disabled. (*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.

4. Maintain organizational policies and processes to ensure that unauthorized media and hardware are not connected to covered assets, such as by limiting use of Universal Serial Bus (USB) devices and removable media or disabling AutoRun. (*NIST CSF 2.0 PR.DS-01, PR.AA-06, & GV.PO-01, CISA CPGs 2.V*)

5. Implement configurations to deny by default 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*)

6. Issue and manage, at an organizational level, identities and credentials for authorized users, services, and hardware, with sufficient attributes available to prevent access of covered data by covered persons or countries of concern. 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 and document a data risk assessment that evaluates whether and how the overall approach selected and implemented pursuant to section II sufficiently prevents access to covered data 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 shall include a mitigation strategy outlining how implementation will prevent access to covered data by covered persons and/or countries of concern. The risk assessment should be reviewed annually 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 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:

1. 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*)

2. 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*)

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 shall 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.

3. Information systems that implement such processing are 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:

1. Comprehensive Encryption: Encrypt covered data in a restricted transaction, regardless of type, during transit and storage using industry-standard encryption. (*NIST Privacy Framework CT.DP-P1, PR.DS-P1, PR.DS-P2, CISA CPGs 2.K*)

2. Transport Layer Security (TLS): Transmit covered data in a restricted transaction over the Internet only using Transport Security Layer (TLS) 1.2 or higher protocols. (*NIST Privacy Framework CT.DP-P1 & PR.DS-P2, CISA CPGs 2.K*)

3. 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 shall not be authorized to have access to encryption keys.

d. All information systems responsible for the storage of and access to encryption keys shall 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:

1. The application of privacy enhancing technologies shall 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).

2. 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*)