Morgan Lewis

REPORT

DOJ'S DATA SECURITY PROGRAM ENFORCEMENT IN FULL SWING:

KEY CONSIDERATIONS FOR COMPANIES

DOJ'S DATA SECURITY PROGRAM ENFORCEMENT IN FULL SWING: KEY CONSIDERATIONS FOR COMPANIES

The US Department of Justice's (DOJ's) final rule implementing Executive Order (EO) 14117, Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern went into effect April 8, 2025. The EO charged DOJ with establishing and implementing a new regulatory program, which is referred to as the Data Security Program (DSP), to address the urgent and extraordinary national security threat posed by the continuing efforts of countries of concern (and covered persons that they can leverage) to access bulk US sensitive personal data and certain US government-related data.

On April 11, 2025, DOJ issued three guidance documents regarding the implementation of the DSP. These documents included (1) an Implementation and Enforcement Policy Through July 8, 2025, (2) a Compliance Guide, and (3) Frequently Asked Questions.

As part of its guidance, DOJ stated that it was exercising its enforcement discretion and would not prioritize civil enforcement of the DSP through July 8, 2025 to allow additional time for individuals and companies to focus on implementation and compliance with the extensive requirements, so long as there was evidence of "good-faith efforts" to do so. However, now that the July 8 deadline has passed, individuals and entities are expected to be in full compliance with the DSP, and DOJ is expected to pursue appropriate enforcement for any violations.

Although DOJ's enforcement priorities have shifted over the past few months, we assess that DOJ fully intends to prioritize enforcement of the DSP. First, we note that the DSP was conceptualized and developed during the Biden administration and has been kept in place by the current US administration even as other Biden administration policies have been significantly modified or discarded. Second, on April 17, 2025, in a bankruptcy-related process usually reserved for matters that implicate the national security equities of the Committee on Foreign Investment in the United States (CFIUS), DOJ's National Security Division submitted a notice to the bankruptcy court to warn that the DSP would prohibit engaging in certain commercial transactions that facilitate the ability of countries of concern or covered persons to access 100 or more US persons' human genomic data and human biospecimens from which human genomic data can be derived.

Now that enforcement of the DSP is in full effect, we summarize below the DSP and key takeaways for individuals and entities potentially impacted by the far-reaching requirements of this comprehensive national security program that will drive how individuals and companies handle certain categories of US sensitive personal data across a number of industries.

Companies are urgently encouraged to do the following:

- Map all collected, processed, or shared data to identify categories of data, check if volumes exceed regulatory bulk thresholds, and determine whether transactions involve countries of concern or "covered persons"
- Implement robust vendor management procedures, often coupled with existing export control and compliance programs, to screen counterparties against national security and sanctions lists
- Establish tailored DSP compliance policies, update internal controls, and train staff to recognize and manage risks under the DSP
- Include clauses in vendor and partner agreements requiring compliance with US data security laws, prohibiting transactions with countries of concern or covered persons, and allowing for audits or suspension if vendors breach obligations
- Engage qualified independent third-party auditors to conduct annual compliance audits covering data transactions, controls, and adherence to security requirements, with detailed reports retained for at least 10 years

- Determine whether exemptions apply to current transactions (e.g., for personal communications, regulatory approvals, or intra-group transfers) and document reliance accordingly; for non-exempt transactions, assess whether to apply for specific DOJ licenses
- For restricted transactions, implement data minimization, encryption, multi-factor authentication, and real-time monitoring to protect sensitive data, aligning with the Cybersecurity and Infrastructure Security Agency's (CISA) security requirements for restricted transactions

KEY ELEMENTS & DEFINITIONS OF THE DSP

DOJ received and reviewed 75 comments in response to the Notice of Proposed Rulemaking (NPRM) that resulted in the Final Rule and DSP from trade associations, public interest advocacy groups, think tanks, private individuals, and companies, as well as comments from several foreign governments. DOJ also reviewed three comments that were relevant to the NPRM and that were timely filed on the docket in response to the CISA *Federal Register* notice requesting comment on proposed security requirements applicable to restricted transactions.

The DSP imposes comprehensive restrictions targeting sensitive personal data transactions with countries and entities posing potential national security risks. Under the DSP, US persons are prohibited from participating in certain data transactions involving specified countries of concern and designated "covered persons."

Countries of Concern (Section 202.601)

The DSP explicitly identifies six countries of concern—**China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela**—that it states (1) engage in a sustained pattern of conduct or serious incidents that are highly detrimental to US national security and the safety of US persons, and (2) pose a significant risk of exploiting government-related or bulk sensitive personal data to harm US national security or the safety of its citizens. Transactions involving bulk sensitive personal data or government-related data with entities tied to these countries would be restricted or prohibited.

As we noted in our prior LawFlash, this definition contrasts with certain other national security regulatory regimes, such as EO 14105 on outbound investment, which named only China; the US Department of Commerce's (DOC's) National Security Guardrails for the CHIPS Program as included in the CHIPS and Science Act, which named only China, Russia, Iran, and North Korea; and DOC's ICTS Connected Vehicle Rule pursuant to EO 13873, which named only China and Russia.

Covered Persons (Section 202.211)

In addition to countries of concern, DOJ will publish a list of "covered persons," adding another layer to existing national security- and sanctions-related lists such as DOC's Entity List, the Treasury Department's Specially Designated Nationals (SDN) List, and the Federal Communications Commission's Covered List.

The DSP defines "covered persons" as being

- an entity at least 50% owned, directly or indirectly, by a country of concern;
- an entity headquartered, organized, or chartered under the laws of a country of concern;
- a foreign individual primarily residing in a country of concern; or
- an employee or contractor of a covered person entity or a country-of-concern government.

Additionally, an entity is deemed a covered person if it is at least 50% owned by another covered person, similar to the Office of Foreign Asset Control's (OFAC's) 50% Rule under its sanctions programs (but also higher than the 25% threshold under the anti-money laundering (AML) program to identify beneficial owners). Notably, only those citizens primarily residing in a country of concern or working for the government of a country of concern or a covered entity are categorically treated as covered persons—other citizens in third countries are not considered covered persons unless specifically designated by the US attorney general.

Covered Data Transactions (Section 202.210)

The DSP covers a range of "data transactions," which include **(1) data brokerage, (2) vendor agreements, (3) employment agreements, and (4) investment agreements**. This approach reflects a shift from, for example, CFIUS's case-by-case approach by applying categorical data security rules that govern foreign investment from a specific type of foreign investor from the outset.

Similar to other regulatory regimes, if a transaction involves an investment agreement that is also a CFIUS-covered transaction, the DSP's security requirements for a restricted transaction would apply until CFIUS takes certain actions to address the data security risks, such as entering into a National Security Agreement. Importantly, CFIUS would explicitly have to designate its action and make clear when an investment agreement is subject to the DSP or CFIUS.

Furthermore, because the DSP focuses on transactions with countries of concern or covered persons, it would not regulate purely domestic transactions between US persons—such as the collection, maintenance, processing, or use of data by US persons within the United States—except to the extent that such US persons are designated as covered persons.

Sensitive Personal Data (Section 202.249)

The DSP identifies six categories of "sensitive personal data" with specific bulk thresholds that would trigger regulation.

Category of Sensitive Personal Data	**Bulk Threshold**
Human Genomic Data and Other Human `Omic (Epigenomic, Proteomic, and Transcriptomic) Data	More than 100 US persons (human genomic data) More than 1,000 US persons (human `omic data)
Biometric Identifiers	More than 1,000 US persons
Precise Geolocation Data	More than 1,000 US persons
Personal Health Data	More than 10,000 US persons
Personal Financial Data	More than 10,000 US persons
Covered Personal Identifiers	More than 100,000 US persons

It should be noted that the DSP revised the NPRM's proposed definition of human biospecimens by excluding human biospecimens intended by a recipient solely for use in diagnosing, treating, or preventing any disease or medical condition. The DSP also changed the reference to human genomic data to human 'omic data to regulate three additional categories of human 'omic data (epigenomic, proteomic, and transcriptomic).

The DSP further made it clear that the term "bulk US sensitive personal data" means a collection or set of sensitive personal data relating to US persons, in any format, regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted, where such data meets or exceeds the applicable "bulk" threshold (set forth in Section 202.205).

The DSP defines "bulk" as any amount of sensitive personal data that meets or exceeds the following thresholds at any point in the preceding 12 months, whether through a single covered data transaction or aggregated across covered data transactions involving the same US person and the same foreign person or covered person.

- **Covered Personal Identifiers (Section 202.212)**: Includes any listed identifier combined with another listed identifier or with other data disclosed in a transaction that links or makes the listed identifier linkable to other listed identifiers or sensitive personal data for 100,000+ individuals
    - However, certain data types are excluded. These exclusions include demographic or contact data that is linked solely to other demographic or contact data, such as names, birthplaces, zip codes, addresses, phone numbers, and email addresses.
    - Additionally, network-based identifiers, account-authentication data, or call-detail data linked only to similar data necessary for the provision of telecommunications, networking, or similar services are also excluded.
- **Precise Geolocation Data (Section 202.242)**: Covers 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 for more than 1,000 US devices
- **Biometric Identifiers** (**Section 202.204)**: Covers data such as facial recognition, voice prints, and retina scans data for 1,000+ persons
- **Human 'Omic Data (Section 202.224)**: Applies to human 'omic data collected about or maintained on more than 1,000 US persons, or, in the case of human genomic data, more than 100 US persons
- **Personal Health Data (Section 202.241)**: Covers personal health data that indicates, reveals, or describes the past, present, or future physical or mental health 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. The definition of "personal health data" includes an illustrative list of the types of data, including 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 involving 10,000+ individuals.
    - DOJ has confirmed that physical and digital dental health records would generally fall within the existing definition of "personal health data" within the scope of sensitive personal data. Additionally, DOJ clarified that this definition encompasses information revealing past, present, or future health conditions.
- **Personal Financial Data (Section 202.240)**: Covers information on an individual's credit, debit cards, bank accounts, and financial liabilities, including payment history, for 10,000+ individuals
- **Government-Related Data (Section 202.222)**: Treated with heightened sensitivity and carrying no minimum bulk threshold requirement, it covers (1) specific government location data to be listed on the DOJ's public Government-Related Location Data List and (2) data linked to current or former US government personnel (including the military and intelligence community, as well as US government contractors)

TRANSACTION PROHIBITIONS, RESTRICTIONS & SECURITY REQUIREMENTS

Prohibited Transactions (Subpart C)

Under Section 202.301, the DSP identifies certain classes of highly sensitive transactions involving data brokerage with countries of concern or covered persons that are categorically prohibited in their entirety.

Section 202.214 defines "data brokerage" as the sale of data, licensing of access to data, or similar commercial transactions involving the transfer of data from any person (the provider) to any other person (the recipient), where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data. The DSP excludes an employment, investment, or vendor agreement for additional clarity.

Restricted Transactions (Subpart D)

The DSP identifies other classes of transactions that would be prohibited except to the extent they comply with predefined security requirements set by CISA to mitigate the risk of access to bulk US sensitive personal data by countries of concern or covered persons.

Furthermore, the DSP provides additional details regarding the "knowledge" element, which under Section 202.305 prohibits US persons from knowingly directing prohibited or restricted transactions.

To illustrate this requirement, the DSP provides multiple examples showing different scenarios, including

- US persons in managerial roles at foreign companies directing prohibited data transactions; and
- US entities with ownership of foreign companies that engage in prohibited data transactions under US direction.

Additional examples in the DSP cover scenarios in which US persons interact with foreign cloud providers or engage with non-covered foreign persons in vendor agreements. If the foreign entity employs covered persons without the US person's knowledge, there is no violation if absent a purposeful evasion of the regulations.

Conversely, transactions such as routine financial services, passive investments, or real estate procurement, where the US person does not direct the covered data transaction activity, are not considered violations. In January 2025, CISA published its security requirements for restricted transactions. In addition to establishing definitions for relevant terms such as "asset," "covered data," and "covered system," the CISA security requirements also provide specific guidance for organizational- and system-level requirements and data-level requirements.

At the organizational and system levels, covered systems (and those who own or operate them) are required to, among other things:

- Have full knowledge and situational awareness of all assets, through identification, prioritization, and documentation, in order to maintain, to the maximum extent practicable, an updated inventory of all covered system assets with each system's respective internet protocol (IP) address; inventory should be updated on a recurring basis, with a no less than monthly occurrence for information technology (IT) assets
- Designate leadership, such as a chief information security officer, to oversee cybersecurity and governance, risk, and compliance (GRC) functions to ensure adherence to these protocols
- Address vulnerabilities, with a mandatory complete remediation timeline of 45 calendar days set for known exploited vulnerability (KEV) issues

- Ensure all contracts with third-party suppliers for covered systems are documented, maintained, and include contractual IT and cybersecurity requirements
- Map network topologies for covered systems to enable real-time monitoring of connections
- Maintain access controls, including multi-factor authentication and immediate revocation of access when personnel roles change, while incident response plans must be regularly updated to handle potential breaches effectively

At the data level, the requirements prioritize:

- Minimizing exposure to sensitive information through data minimization and masking techniques such as aggregation, pseudonymization, and anonymization; such methods reduce the risk of unauthorized access to identifiable information
- Applying encryption techniques as a cornerstone of the data protection strategy, with all sensitive data required to be encrypted during transmission and storage; only secure, industry-standard protocols, such as TLS 1.2 or higher, are considered comprehensive, and encryption keys must be carefully managed and stored separately from the data itself
- Employing privacy-enhancing technologies, including homomorphic encryption, to prevent data reconstruction or linkage to US persons, thereby maintaining privacy even in data analysis scenarios
- Stringent identity and access management practices to restrict data access to only authorized personnel and exclude countries of concern

Exemptions (Subpart E), Licensing (Subpart H) & Advisory Opinions (Subpart I)

The DSP contains specific exemptions for transactions incidental to routine business or those complying with other federal regulations. Companies across various industries should consider leveraging the available exemptions, which cover several transaction types.

Subpart E Exemptions (Sections 202.501–202.511)

- **Personal Communications (Section 202.501)**: Exempts data transactions involving non-commercial personal communications, such as postal, telephonic, or telegraphic exchanges, that do not transfer items of value
- **Information or Informational Materials (Section 202.502)**: Exempts the import or export of information or materials, irrespective of format or transmission method, whether for commercial or non-commercial purposes
- **Travel (Section 202.503)**: Exempts data transactions related to personal travel, including importing personal baggage, covering living expenses, and facilitating travel arrangements
- **Official US Government Business (Section 202.504)**: Exempts transactions for official government purposes, such as federal grants or contracts, provided they are aligned with specified official activities
- **Financial Services (Section 202.505)**: Exempts transactions incidental to financial services, such as banking, payments, investment management, and fraud prevention, provided they are integral to these services
- **Corporate Group Transactions (Section 202.506)**: Exempts intra-group transactions between a US person and its affiliates or subsidiaries in countries of concern, provided the data exchange supports administrative or ancillary business functions like HR, payroll, compliance, or customer support
- **Federal Law- or International Agreement-Authorized (Section 202.507)**: Exempts transactions required or authorized by federal law or international agreements, including global health and pandemic preparedness frameworks

- **CFIUS-Regulated Transactions (Section 202.508)**: Exempts data transactions tied to investment agreements subject to actions by CFIUS, including mitigation agreements
- **Telecommunications Services (Section 202.509)**: Exempts data transfers integral to telecommunications services, such as those necessary for international roaming or network provisioning but excludes unrelated data sales
- **Drug, Biological Product, and Medical Device Authorizations (Section 202.510)**: Exempts data necessary for regulatory approval or maintenance of authorization to market or research medical products, provided it complies with de-identification standards
    - To clarify about whether this exemption would apply to the use of an agent/vendor/employee located in a country of concern tasked with submitting approval data to country of concern regulators, the DSP makes it clear that sharing regulatory approval data in those instances is permitted. Therefore, a registered agent, country of concern subsidiary of a US company, or an employee of a US company who primarily resides in a country of concern that will be submitting approval data to a country of concern regulator, as required by a country of concern's laws, is exempt because it is "necessary" to obtain an approval or authorization. In contrast, entering into a vendor agreement with a covered person to store and organize regulatory approval data for eventual submission to a country of concern regulator is not "necessary" to obtain regulatory approval if it is not required by a country of concern's laws.
- **Clinical Investigations and Post-Marketing Data (Section 202.511)**: Exempts data related to FDA-regulated clinical investigations, real-world safety data, and post-marketing surveillance for drugs, biological products, devices, and infant formula as long as the data is de-identified or pseudonymized

Subpart H Licensing (Sections 202.801–202.803)

For transactions that do not meet these exemptions, the DSP authorizes DOJ to issue specific licenses for specific transactions by parties who apply for and disclose details of their intended transactions in a license application. The DSP sets out the requirements and procedures for the issuance of general and specific licenses, including the process to apply for a specific license or seek reconsideration of a denied license based on new information.

Category	Summary
General License (Section 202.801)	Issued by the US attorney general with concurrence from the secretaries of State, DOC, and Homeland Security. Authorizes categories of transactions involving sensitive personal data that would otherwise be prohibited. These apply broadly and do not require an application.
Specific License (Section 202.802)	May be granted upon application to authorize a particular transaction or set of transactions not otherwise covered by a general license. Also requires DOJ concurrence with State, Commerce, and DHS before issuance, amendment, or revocation. Applicants for specific licenses must describe the transaction's data types, parties, end-use, and transfer methods. Only one copy should be submitted, and additional information may be requested. DOJ aims to respond within 45 days.

	Licenses are limited to named parties, specified data, and stated conditions.
General Provisions (Section 202.803)	The US attorney general may exclude any person, property, or transaction from the scope of any license or from the privileges conferred by a license. The US attorney general may restrict a license's applicability to particular persons, property, or transactions (or classes thereof). All license actions (issuance, amendment, and revocation) require concurrence of DOJ, State, Commerce, and DHS.

Subpart I Advisory Opinions (Section 202.91)

Similar to other regulatory regimes, the DSP permits DOJ to issue public guidance to address frequently asked questions and common issues, as well as advisory opinions to address the applicability of the regulations to specific transactions (must involve actual specific transactions, not hypothetical situations).

Subparts J & K Due Diligence, Audit & Reporting, and Recordkeeping Requirements (Sections 202.1001–202.1002 and 202.1101–1104)

The DSP emphasizes rigorous compliance measures, urging US persons engaging in restricted transactions to develop individualized compliance programs that reflect their risk profile. Specifically, by no later than October 6, 2025, US persons that engage in restricted transactions are required to develop and implement a data compliance program and conduct audits. Affirmative compliance measures include:

- **Recordkeeping and Due Diligence**: Companies must maintain transaction records, including sensitive data types, data flow logs, and vendor information, with records retained for 10 years
- **Auditing**: Independent annual audits to verify compliance with CISA's cybersecurity standards

And to enhance oversight and ensure that US persons are accountable in managing data-related transactions, the DSP sets forth specific reporting requirements throughout various provisions. For example, key reporting obligations include:

- **Annual Reports (Section 202.1103):** US persons involved in restricted transactions with cloud-computing services that are at least 25% owned, directly or indirectly, by a country of concern or a covered person must submit annual reports by March 1 of the subsequent year
- **Reports on Rejected Prohibited Transactions (Section 202.1104):** Any US person who has received and explicitly declined an offer to engage in a prohibited transaction involving data brokerage is required to file a report
- **Reporting Known or Suspected Violations (Section 202.302):** US persons engaged in data brokerage transactions with foreign non-covered persons must report if they know or suspect the foreign counterparty is violating restrictions on resale or onward transfer to countries of concern or covered persons
- **Exemption Invocation Reports (Sections 202.510, 202.1101(a), and 202.1102):** US persons claiming an exemption for data transactions necessary for regulatory approval to market a drug, biological product, device, or combination product in a country of concern must report these activities

Recognizing that US persons may need more time to amend internal policies and procedures to ensure compliance with the DSP's due diligence provisions and to comply with reporting requirements, compliance with certain provisions, including due diligence and audit requirements under Subpart J and specific reporting requirements under Sections 202.1103 and 202.1104 of Subpart K for restricted transactions, will be delayed until October 6, 2025. Multinational companies that already have robust data privacy, data security, and export control programs can leverage adapting their existing compliance programs to respond to the DSP requirements.

Subpart M Penalties & Finding of Violation

Violations of the DSP may trigger significant civil and criminal penalties under the International Emergency Economic Powers Act (IEEPA). Civil penalties can reach the greater of $368,136 or twice the value of the transaction and are subject to inflation adjustments. Willful violations may result in criminal prosecution, with penalties including fines up to $1 million and imprisonment of up to 20 years. False statements related to any filing or interaction with the DOJ may also result in separate criminal liability under 18 USC § 1001.

Generally speaking, DOJ initiates enforcement by issuing a pre-penalty notice describing the alleged violation and proposed fine, to which the recipient has a right to respond within 30 days. If a violation is confirmed, DOJ may issue a final penalty notice, which constitutes final agency action and can be challenged in federal district court. Unpaid penalties may be referred to the US Treasury for collection or pursued in court.

In cases in which DOJ finds a violation occurred but determines a monetary penalty is not the most appropriate response, it may issue a finding of violation instead. This written notice formally documents the misconduct and allows the alleged violator an opportunity to respond. A final finding of violation may be issued after review, and the finding constitutes final agency action and is subject to judicial review. Both pre-penalty and violation findings can be contested by submitting supporting documentation and arguments.

PRACTICAL TIPS

To comply with the DSP, companies should first assess whether their operations involve sensitive personal data or government-related data as defined under the rule. It is critical to identify any transactions or relationships involving countries of concern, such as China, Russia, Iran, North Korea, Venezuela, or Cuba, as well as entities or individuals classified as "covered persons." A thorough data mapping exercise is essential to classify the types of data collected, processed, or shared. This process should identify whether any data volumes exceed the defined bulk thresholds for sensitive personal data categories, such as biometric identifiers, geolocation data, or personal health information.

Additionally, companies should implement vendor management validation procedures to screen all third parties against national security and compliance lists, including the Specially Designated Nationals (SDN) List, Entity List, Covered List, and other relevant sanctions lists. This screening ensures that companies do not inadvertently engage in restricted transactions with prohibited parties and strengthens overall compliance with the DSP requirements.

Companies should also evaluate their supply chains and business partnerships to assess whether they involve "covered persons" or entities tied to countries of concern. If so, companies should determine whether any applicable exemptions exist—such as exemptions for certain telecommunications or financial services—or whether they can make a compelling case to seek a specific license to be allowed to continue engaging in the prohibited or restricted transaction. Implementing robust due diligence protocols for third-party relationships can mitigate risks associated with restricted transactions and prevent inadvertent regulatory violations. Any gaps identified in vendor or partner compliance should be addressed promptly.

Companies should also consider developing a tailored compliance program to include policies and procedures for identifying restricted transactions, monitoring compliance, and reporting activities. Training employees who manage data transactions is also important to ensure they understand the new obligations and can identify potential risks in day-to-day operations.

Companies should also consider including robust contractual provisions in agreements with third parties, vendors, and service providers. Such provisions should (1) require adherence to US data security laws and regulations; (2) mandate that vendors not engage in prohibited transactions with countries of concern or with entities designated as "covered persons"; (3) include rights to audit, terminate, or suspend services if the vendor fails to comply; and (4) require vendors to implement security measures consistent with CISA-recognized encryption protocols.

For US persons engaged in restricted transactions, compliance obligations include working with a qualified, independent third-party auditor (i.e., one not affiliated with any covered person or country of concern). The auditor must annually review restricted transactions, the company's data compliance program, required records, and its adherence to CISA's security requirements. The audit must cover the preceding 12 months and result in a detailed written report within 60 days of completion. This report must outline the nature of restricted transactions, describe the audit methodology, assess the effectiveness of the compliance program, and identify any vulnerabilities or security failures. It must also recommend remedial actions and be retained for at least 10 years.

Given the rigor of the auditing requirements, organizations should consider strengthening cybersecurity and data protection measures, even if their transactions are not currently classified as prohibited or restricted. This includes implementing encryption protocols recognized by CISA for sensitive data, including, among others, enforcing multi-factor authentication (MFA) for system access (or passwords with sufficient strength where MFA is not technically feasible and/or not enforced), as well as establishing real-time monitoring of data flows and network activity. Regular updates to incident response plans and vulnerability management processes will ensure the organization is prepared to address potential breaches.

The DSP's impact is reflected by the broad swath of industries its requirements implicate—regardless of the level of sophistication or relative size—simply based on the types of data involved and whether the transactions identified expose those data to countries of concern or covered persons. That said, the DSP will have substantial implications for multinational companies headquartered in countries of concern that have operations in the United States, as well as the US persons with which they have commercial relationships.

Key sectors affected may include

- companies relying on large-scale data training for artificial intelligence (AI) development;
- businesses leveraging third-party data brokers to acquire bulk user data for targeted advertising initiatives; and
- business-to-consumer (B2C) companies—such as those in the automotive, e-commerce, healthcare, AI, and robotics industries—whose products or services require the collection of sensitive US personal data with subsequent transfer to overseas headquarters for processing.

These companies should promptly assess their data flows and establish a practical compliance pathway, which includes ensuring adherence to CISA requirements, conducting thorough due diligence, maintaining robust recordkeeping practices, and performing compliance audits with third-party independent auditors. Documenting the reliance on exemptions and ensuring compliance with their specific conditions is essential to avoid regulatory challenges. For transactions that do not qualify for exemptions, organizations should prepare to engage with DOJ's licensing process. This involves gathering the necessary documentation and applying for specific licenses, as well as monitoring updates or guidance from DOJ regarding the rule's implementation.

Finally, organizations should take advantage of the second transition period, until October 6, to implement further necessary changes. This time should be used to update internal policies, train employees, and establish compliance mechanisms. The DSP's annual recordkeeping and audit requirements will entail ongoing obligations. Noncompliance presents a heightened risk for entities whose data sets fall within the aforementioned categories and whose business models potentially qualify as prohibited or restricted transactions. Engaging legal and compliance experts during this process can provide additional guidance and help ensure readiness by the applicable deadlines.

Two of the authors of this report, David Plotinsky and Loyaan Egal, previously led DOJ's Foreign Investment Review Section (FIRS), which has been charged by DOJ with developing and implementing the DSP.

CONTACTS

If you have any questions or would like more information on the issues discussed in this report, please contact any of the following:

Authors

Loyaan A. Egal	+1.202.739.5941	loyaan.egal@morganlewis.com
David Plotinsky	+1.202.739.5742	david.plotinsky@morganlewis.com
Jiazhen (Ivon) Guo	+1.202.739.5163	ivon.guo@morganlewis.com

Beijing

Bingna Guo	+86.10.5876.3588	bingna.guo@morganlewis.com

Boston

Heather Egan	+1.617.341.7733	heather.egan@morganlewis.com

Philadelphia

Ezra D. Church	+1.215.963.5710	ezra.church@morganlewis.com
Kristin M. Hadgis	+1.215.963.5563	kristin.hadgis@morganlewis.com
Gregory T. Parks	+1.215.963.5170	gregory.parks@morganlewis.com

Shanghai

Todd Liao	+86.21.8022.8799	todd.liao@morganlewis.com
Sylvia Hu	+86.21.8022.8527	sylvia.hu@morganlewis.com

Washington, DC

Hannah Levin	+1.202.739.5896	hannah.levin@morganlewis.com
Sandra Moser	+1.202.739.5393	sandra.moser@morganlewis.com
Justin D. Weitz	+1.202.739.5932	justin.weitz@morganlewis.com
Dr. Axel Spies	+1.202.739.6145	axel.spies@morganlewis.com

Morgan Lewis

At Morgan Lewis, we're always ready to respond to the needs of our clients and craft powerful solutions for them.

Connect with us

www.morganlewis.com

070325_251317