# DOJ Issues Guidance for New Data Security Program

APRIL 18, 2025

On April 8, the Department of Justice's ("DOJ's") final rule on *Preventing Access to US Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons* (the "Rule") formally took effect. Issued pursuant to President Biden's 2022 Executive Order ("E.O.") on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern (EO 14117), the Rule imposes broad restrictions on the access of US sensitive personal data and government-related data to certain covered countries of concern and covered persons, as well as a suite of new compliance and reporting requirements across industries. The Rule also creates a new Data Security Program ("DSP") within the DOJ's National Security Division ("NSD") to oversee implementation, including through issuance of licenses and advisory opinions.

On Friday, April 11, the NSD issued much anticipated guidance on the Rule's implementation, including (i) an overarching implementation and enforcement policy for the program ("Enforcement Policy") through the next 90 days; (ii) a 21-page Compliance Guidance; and (iii) a 45-page guide to frequent answers and questions ("FAQs"). Moreover, the NSD previewed that additional guidance would be forthcoming in the coming weeks regarding an initial Covered Persons List that identifies and designates persons subject to the control and direction of foreign adversaries.

We have previously written about the Rule in a Jan. 23, 2025, client alert ("DOJ Finalizes Rule Regarding Sensitive Data Transfers"), and recently did a brief April 10 webinar ("What You Need to Know About the DOJ's Sensitive Data Access Rule") providing an overview of the Rule and key provisions, as well as compliance strategies given the current priorities of the Trump Administration.

The following post provides a high-level summary of these new guidance documents, along with our top takeaways so far.

**Key Takeaways**:

1. **Regulating data transfers will remain a bipartisan priority—and may even accelerate under the Trump Administration.** As it revisits other Biden-era rules, the NSD's recent guidance emphasizes its "continued prioritization of the Data Security Program," and traces

a throughline from Trump's recent Presidential proclamations to his 2017 National Security Strategy, which described the People's Republic of China's ("PRC's") willingness to weaponize US person data.

2. **Compliance started "yesterday."** Despite calls from industry, the NSD has declined to delay enforcement of the new Rule, urging companies to immediately "know your data." While the NSD has indicated that it will not "prioritize civil enforcement actions" over the next 90 days for those US persons engaging "in good faith efforts to comply with or come into compliance with the Data Security Program," it will nonetheless focus on "egregious, willful violations." At the end of this 90-day period, the NSD moreover expects that individuals and entities should be "in full compliance," though certain affirmative obligations, including auditing requirements for restricted transactions and reporting obligations for restricted or rejected prohibited transactions, do not come into effect until October 2025.
3. **Licenses aren't a near-term option—and will be presumptively denied.** While the Rule envisions that the NSD may issue specific licenses permitting certain data transfers, the NSD has proactively discouraged companies from seeking specific licenses, or formal advisory opinions over the next 90 days—emphasizing that they will not be reviewed or adjudicated. Going one step further, the NSD says in the Compliance Guide that it will apply *a presumption of denial standard to all specific license applications*—which the Rule notably did not indicate. Nonetheless, the NSD has encouraged the public more broadly to contact the NSD with "informal queries" to develop and refine future guidance—a testament to the fact that the NSD appreciates the Rule's complexity.
4. **Compliance processes will vary, and there's no safe harbor.** The NSD's Compliance Guide emphasizes that "the failure to adopt and maintain adequate data compliance policies and procedures is potentially a violation...and may be an aggravating factor in any enforcement action." That said, the NSD has emphasized that whether a compliance program satisfies the DSP requirements is likely to be a highly fact-dependent, holistic inquiry that considers "the US persons' size and sophistication, products and services, customers and counterparties, and geographic locations." While the Compliance Guide provides baseline suggestions for what a strong compliance regime might include, it's explicit in stating that adherence to those standards does not provide companies with safe harbor.
5. **Companies should exercise caution when assessing who qualifies as a covered person under the Rule.** Under the Rule, transactions including data brokerage with countries of concern and covered persons are prohibited, absent an exemption or valid license. While the NSD intends to publish a copy of the designated "covered persons list" in the near future, the division has communicated that it is not going to be an exhaustive list upon which companies can entirely rely—requiring ongoing due diligence. Companies do not have a formal obligation to determine control of the counterparties with which they do business—as opposed to direct and indirect ownership in the aggregate at 50% or more—but the NSD nonetheless has cautioned that US persons should exercise caution where covered entities may exercise "significant control." Moreover, as the FAQs explain in detail, *the Rule treats ownership percentages in the aggregate across multiple covered persons.*
6. **The NSD is taking a totality-of-the-circumstances approach to assessing violations, to**

**include active participation by senior company management.** The NSD appears to recognize that full compliance with the Rule may take time, and it states that it will consider all relevant facts and circumstances in the event of a violation, including the relative sophistication of the individuals or entities at issue. The NSD's guidance repeatedly emphasizes that senior management—to include C-suite and Board-level officials—must be involved in establishing robust compliance programs. It seems likely that, at least initially, robust and good-faith efforts by company leadership to comply with the new program could help stave off early enforcement actions.

7. **Meanwhile, other "data security" compliance obligations may still apply.** Consistent with its explanation in the Rule, the NSD's FAQs clarify how the Rule intersects with other regulatory requirements under the Committee on Foreign Investment in the United States ("CFIUS"), the Department of Commerce's Information and Communications Technology and Services ("ICTS") authorities, and the Protecting Americans' Data from Foreign Adversaries Act of 2024 ("PADFAA"). In the case of Commerce's ICTS authorities under E.O. 13873, the NSD clarified that it regards the Rule as creating a "floor," while still permitting Commerce to take more stringent actions against a specific vendor, transaction, or class of ICTS beyond those requirements by the Rule. In the case of CFIUS, the NSD states that the security requirements regulating US persons' engagements in a restricted transaction apply "until and unless" CFIUS takes actions to address data security risks through a migration agreement. At that point, the security requirements created by the Rule would no longer apply.
8. **The NSD doesn't have much additional clarification on the application of critical exemptions.** While reinforcing that certain transactions otherwise prohibited or restricted may qualify for an exemption, the NSD does not otherwise provide much additional insight into how those exemptions function. For example, the FAQs include just one question about the corporate group transaction—likely the most relevant to broad swaths of industry—to clarify that it doesn't apply to routine research or development activities. The NSD provides no further examples wherein the corporate group transaction *would apply*, though it reaffirms that the administrative and ancillary business activities listed in the exemption are not exhaustive.

## Summary of Key Documents

### Enforcement Policy

The NSD's Enforcement Policy indicates that while the implementation of the DSP is intended to take immediate effect, the agency will not prioritize enforcement where a person (e.g., individual or company) has engaged in "good-faith efforts" to comply, or come into compliance, with the program for the first 90 days from the program's implementation (April 8, 2025 through July 8, 2025). Voluntary cooperation to NSD inquiries will also be "favorably considered" in considering civil enforcement. However, during this time, enforcement actions may still be brought within the first 90 days of the program's implementation for "egregious, willful violations."

Indications of "good-faith efforts" may include:

- conducting internal reviews of access to data, internal datasets, and datatypes to determine DSP applicability;
- conducting a review of vendors and vendor agreements or negotiating contracts;
- negotiating contractual onward transfer provisions with foreign persons who are the counterparties to data brokerage transactions;
- adjusting employee work locations, roles, or responsibilities;
- evaluating investments and investment agreements from countries of concern or covered persons; or
- implementing the Cybersecurity and Infrastructure ("CISA") Security Requirements for Restricted Transactions.

Finally, as reiterated in the Enforcement Policy and pursuant to the Rule, persons are not required to immediately comply with the DSP's affirmative obligations related to due diligence and audit requirements for restricted transactions, reporting requirements for certain restricted transactions, or reporting requirements on rejected prohibited transactions until October 6, 2025 (as indicated in 28 C.F.R. Part 202, Subpart J, 28 C.F.R. § 202.1103, and 28 C.F.R. § 202.1104). According to the Rule, the additional six-month extension is to provide sufficient time to phase in additional compliance requirements associated with an assessment of data transactions, updates of internal policies to comply with reporting requirements, and making necessary data security changes without disrupting commercial activity.

Pursuant to the International Emergency Economic Powers Act ("IEEPA"), the DOJ is authorized to bring civil enforcement actions and criminal prosecutions for knowing or willful violations of the program's requirements. Civil penalties may be up to the greater of $368,136 or twice the value of each violative transaction, whereas criminal ("willful") violations of the IEEPA are punishable by imprisonment of up to 20 years and a $1,000,000 fine.

## Compliance Guide

-

The DSP Compliance Guide identifies and describes best practices for complying with the program, including guidance on key definitions, prohibited and restricted transactions, and the requirements for building a robust data compliance program. The Compliance Guide offers several important clarifications about the NSD's expectations for the DSP's implementation and exemptions.

1. Notable Requirements, Clarifications, and Best Practices

First, a data brokerage contract between US persons and *any non-covered foreign person or entity must include language prohibiting that foreign person or entity* from engaging in the onward transfer or sale of covered data to countries of concern or covered persons—a non-covered middleman does not satisfy the DSP. As previewed in the Rule, the Compliance Guide includes some model contractual language to prohibit the onward sale or transfer from foreign persons to covered persons, while noting that parties may choose to tailor their contractual language according to the relevant business activity. The Compliance Guide also suggests that contracts require periodic certification of compliance by the non-covered foreign persons and provides model language to that effect. The Compliance Guide additionally makes clear that shifting compliance entirely to the foreign person is insufficient to avoid enforcement actions—the US person must maintain ongoing due diligence measures.

Second, US persons must establish Data Compliance Programs that include (1) internal controls for *logging and verifying* the type and volume of covered data in any restricted transaction, the identity of the transacting parties, and the end-use of the data and method of transfer; (2) written policies and procedures that are annually certified; and (3) annual audits. It also recommends at least annual risk assessments and training programs, and it offers specific examples of the type of material to include in such assessments and programs. While not required, these types of measures will be part of the circumstances that DOJ evaluates in the event of a violation. And though the NSD will publish a Covered Persons List for entities or persons that it specifically designates, the List may not include all those who are nonetheless subsumed within the definitions of "covered persons" in the DSP. In other words, US persons cannot rely solely on the Covered Persons List to ensure compliance. The Compliance Guide offers suggestions for the types of controls a US entity's screening software should include to ensure

compliance. However, the NSD specifies that for vendor agreements with foreign entities, US persons do not need to conduct due diligence on the employment practices of those foreign entities to ensure none of the foreign entities' employees are covered persons (unless such an arrangement is a knowing attempt to evade the DSP's restrictions).

As for the required annual audits, auditors must be independent and disassociated with the covered transactions and transacting parties. However, the DSP does not require a separate audit, nor does it require a specific auditing standard. Rather, audits that are completed for other purposes will suffice, so long as they specifically, sufficiently, and expressly address the DSP's requirements and adhere to an appropriate and reliable methodology.

Third, the record-keeping requirements apply to non-exempt covered data transactions, covered transactions authorized by general or specific licenses (which may include additional reporting requirements), and transactions concerning certain drug, biological product, and medical device authorizations. There are also certain annual reporting requirements and ad hoc reporting requirements as directed by the NSD, though this requirement does not take effect until October 6, 2025.

2. Senior Management Responsibilities

Involvement and buy-in from senior management are not only recommended but, in some circumstances, required to comply with the DSP. US companies should appoint a compliance manager with appropriate resources, staffing, and seniority to implement and test the companies' Data Compliance Programs. That employee or an officer or executive should sign annual certifications of (1) the Data Compliance Program implementation

and due diligence efforts; (2) implementation of any supplemental security requirements; and (3) the completeness and accuracy of recordkeeping, as supported by an audit. The NSD strongly suggests that the certification process be used as an opportunity for senior management to assess the company's Data Compliance Program. The NSD also suggests that the certification should report whether the CEO, board of directors, and audit committee have reviewed the Data Compliance Program, whether compliance personnel have met with the CEO in the last year, and whether the CEO has consulted with compliance personnel and any outside entities to verify the content of the certification.

3. Exemptions, Licensing, and Advisory Opinions

Subpart E of the DSP outlines several categories of exempt transactions, including those conducted as part of official US government business, financial services, intra-corporate group transfers, and specific health-related activities (e.g., clinical trials). Transactions falling under these exemptions are not subject to the core prohibitions or affirmative compliance requirements (subparts C, D, J, K), though reporting and recordkeeping may still apply. Additionally, the NSD may authorize otherwise prohibited transactions via general or specific licenses. General licenses are self-executing, while specific licenses require application and are subject to a "presumption of denial" standard. Applicants must demonstrate compelling national security or public safety justification to overcome this presumption. During the 90-day forbearance period, the NSD encourages entities to seek informal guidance via email, but it discourages US persons from seeking specific licenses as they will not be adjudicated. Moreover, the NSD will offer advisory opinions to potentially regulated entities upon request to help guide compliance, even after the 90-day forbearance window.

## FAQs

The FAQs address high-level deadlines, outline enforcement priorities and the scope of the DSP. These deadlines are consistent with those laid out in the Rule and aforementioned Enforcement Policy, aside from NSD's near-term enforcement priorities.

***Enforcement Priorities:*** As discussed, NSD will target its enforcement efforts during the first 90 days to allow US persons (e.g., individuals and companies) additional time to continue implementing the necessary changes to comply with the DSP and provide additional opportunities for the public to engage with NSD on DSP-related inquiries. Further, informal inquiries rather than formal requests for specific licenses are permitted during the period from April 8, 2025 through July 8, 2025.

***Scope:*** The prohibitions of DSP do not address purely domestic data transactions between non-covered US persons. The prohibitions do not apply in instances where a US person accesses data from a covered person. In other words, the DSP applies only if a transaction involves risk of a country of concern or covered person obtaining access to government-related data or bulk US sensitive personal data. The affirmative requirements of the Rule are tailored such that persons subject to US jurisdiction must implement a compliance program tailored to their individualized risk profile.

***Corporate Group Transactions Exemptions:*** In general, data transactions are exempt from the rule to the extent they are (1) between a US person and its subsidiary or affiliate located in (or otherwise subject to the ownership, direction, jurisdiction, or control of) a country of concern; and (2) ordinarily incident to and part of administrative or ancillary business operations (such as sharing employees' covered personal identifiers for

human-resources purposes); payroll transactions (such as the payment of salaries and pensions to overseas employees or contractors); and paying business taxes or fees. The FAQs highlight that research and development conducted by US companies with corporate affiliates in countries of concern is not exempt under § 202.506.

***Interplay with CFIUS:*** In instances where a transaction involves an investment agreement that is also a covered transaction subject to CFIUS's review, the DSP's requirements regulating US persons' engagement in a restricted transaction apply until and unless CFIUS explicitly designates its action as a "CFIUS action."

***Hiring, contracting with, or accepting investments from covered persons or countries of concern:*** The DSP does not categorically prohibit the US company from offering employment to covered persons. For example, a US business that holds bulk US sensitive personal data could accept an investment from a covered person or hire a covered person as a board director (a restricted transaction) by complying with the security requirements to deny or otherwise mitigate the covered person's access to that data.

***Audits:*** Companies can use audits completed for other purposes to comply with the DSP. Additionally, the DSP permits US persons to satisfy the requirements of § 202.1002 (Audits for restricted transactions) by conducting internal audits.

***Licenses:*** To authorize otherwise prohibited activity, the NSD will issue general licenses and specific licenses. A general license authorizes a particular type of transaction for a class of persons. Specific licenses are issued to a particular individual or entity authorizing a particular transaction

(or transactions) subsequent to a written license application. The NSD will determine and issue, at its discretion, general licenses in particular circumstances, such as where multiple companies in the same industry submit requests for specific licenses on the same topic, or in circumstances where the NSD otherwise learns of a need to issue a general license, such as through industry engagement. Specific license applications will be reviewed on a case-by-case basis. In general, to overcome what has been announced as a presumption of denial, a license application will need to affirmatively identify compelling countervailing considerations to support the issuance of a specific license (such as an emergency or imminent threat to public safety or national security).

***Annual Reports:*** An annual report is not required for all US persons. Only US persons that, on or after October 6, 2025, are engaged in a restricted transaction involving cloud computing services, and that has 25% or more of the US person's equity interests owned (directly or indirectly, through any contract, arrangement, understanding, relationship, or otherwise) by a country of concern or covered person.

***Obligation to identify covered persons:*** Under § 202.211(a), the four categories of covered persons, which exclude US persons, are: (1) foreign entities headquartered in or organized under the laws of a country of concern; (2) foreign entities 50% or more owned by a country of concern or covered person; (3) foreign individuals primarily resident in a country of concern; and (4) foreign individuals who are employees or contractors of a covered person entity or a country-of-concern government.

To assist in compliance, the NSD may identify some covered persons on its non-exhaustive Covered Persons List. The FAQs note that the Covered

Persons List is accessible through the following page on the NSD's website at *https://www.justice.gov/nsd*. [However, no list is publicly available as of April 17, 2025.]

US persons are obligated to take reasonable steps, as part of a risk-based compliance program, to ascertain whether other individuals and entities fall into one or more of those categories as listed above. The NSD may also designate any person (including a US person) as a covered person based on certain criteria such as being subject to the ownership or control of a country of concern. Designated covered persons remain covered persons even when located in the United States.

## *Authors*


**Jason C. Chipman**
PARTNER

jason.chipman@wilmerhale.com
+1 202 663 6195

**Arianna Evers**
PARTNER

arianna.evers@wilmerhale.com
+1 202 663 6122

**Hilary A. Hurd**
SENIOR ASSOCIATE

hilary.hurd@wilmerhale.com
+1 202 663 6373

**Shervin Z. Taheran**
ASSOCIATE

shervin.taheran@wilmerhale.com
+1 202 663 6268

# Sarah Litwin

**ASSOCIATE**


sarah.litwin@wilmerhale.com

+1 617 526 6288