View on our website.

DOJ Data Security Program Task Force Update October 24, 2025

Gibson Dunn DOJ Data Security Program Task Force Update – Final Provisions of the DSP Come into Effect

Gibson Dunn lawyers are advising clients across sectors in building and validating their DSP compliance programs. We remain closely engaged with evolving guidance and agency posture and are available to assist in addressing any questions you may have about these developments and your own DSP readiness.

Final provisions of the DOJ's audit, recordkeeping, and reporting obligations came into effect on **October 6, 2025**; accordingly, companies are now expected to have fully implemented and operationalized a DSP compliance program relating to access by countries of concern to U.S. bulk sensitive personal data.

While many of these requirements apply specifically to companies who engage in restricted transactions, notably, reporting requirements for rejected transactions that involve data brokerage apply to **all U.S. Persons** – making an understanding of the October 6th obligations critical to the compliance efforts of all U.S. companies.

Background

- On **December 27, 2024**, the Department of Justice (DOJ) issued a final rule pursuant to **Executive Order 14117** that established a new federal regulatory framework imposing restrictions on transactions that could provide certain persons with access to **"bulk sensitive personal data"** and **"United States government-related data."**[1] This

regulatory framework, which came into effect on **April 8, 2025**, is referred to by DOJ as the **Data Security Program (DSP)**.[2]

- The DSP restricts or prohibits certain transactions that could involve access to bulk U.S. sensitive personal data or U.S. government data by covered persons and countries of concern (most notably, China), and imposes **diligence, security, audit, and recordkeeping requirements**.

- Violations of the DSP carry significant potential penalties, including **civil penalties** up to the greater of **$377,700** or **twice the value of the transaction** and/or **criminal penalties** up to **$1 million** and **20 years' imprisonment** for willful violations.

- A **90-day de-prioritization of civil enforcement** for entities making "good faith" compliance efforts expired on **July 8, 2025**. DOJ now expects that "individuals and entities should be in full compliance with the DSP and should expect [the DOJ National Security Division] to pursue appropriate enforcement with respect to any violations."[3]

Requirements as of October 6, 2025

As of **October 6, 2025,** DSP provisions have come into effect requiring companies engaging in restricted transactions to meet certain ongoing **operational compliance obligations**, including **audit program implementation**, **reporting and certification requirements**, and **long-term recordkeeping**.

Key requirements for U.S. companies engaged in restricted transactions that are now in effect include:

- **Audits for restricted transactions:** All U.S. Persons that engage in restricted transactions on or after October 6, 2025, must conduct a comprehensive audit, using an independent auditor that is neither a covered person nor from a country of concern.

    - The audit must be scoped to cover (1) the restricted transactions; (2) assessment of the data compliance program (discussed in detail below) and its implementation; (3) review of relevant records; and (4) examination of required security controls.

    - The audit must be conducted by an independent auditor. This independent auditor "should be objective, fact-based, nonpartisan, and nonideological with regards to both the U.S. person and to the transactions that are subject to the audit."[4] While DOJ permits U.S. companies to use internal auditors to audit compliance with the DSP, it cautions that many internal audits in the national security, criminal, and other contexts lack the necessary independence of external audits.[5] Even when a U.S. company uses an external auditor, DOJ could reasonably question the objectivity of such an audit if the company uses the same firm to build and audit its compliance program.

    - The audit must be completed once for each calendar year in which the U.S. person engages in any restricted transactions and must cover the preceding 12 months, in addition to certain other requirements with respect to the scope and auditor qualifications.[6] For those companies who have engaged in a restricted transaction since the DSP regulations first came into effect in April 2025, this means that an audit must be completed by the end of the 2025 calendar year.

    - The audit must be maintained by the company for a period of 10 years, but is not automatically required to be submitted to DOJ.[7]

- **Recordkeeping:** U.S. Persons must also preserve the records associated with any restricted transactions for at least 10 years, including the due diligence conducted to verify restricted transaction data flows, the types and volume of data involved, the transaction parties, the dates of the transaction, the method of data transfer and other details of the transaction and end-use of the data. In addition, records must be retained regarding required compliance measures, including copies of applicable data compliance program policies, audit results, and any relevant licenses or advisory opinions.[8]

- **Annual reports for companies partially owned by a covered person or country of concern and that engage in restricted cloud computing transactions:** As of October 6, 2025, U.S. Person companies that (1) engage in restricted transactions involving cloud computing services, and (2) are 25% or more owned by a country of concern or covered person, must file annual reports with DOJ. This report, among other requirements, must include detailed information on the transacting entity, the restricted transaction, and any relevant documentation created in connection with the transaction.[9]

U.S. Person companies that engage in restricted transactions must have a fully implemented **data compliance program**, including:

- Risk-based procedures for verifying data flows involved in any restricted transaction, and for verifying and logging certain key metrics and data points;

- For transactions involving vendors, risk-based procedures for verifying the identity of vendors;

- A written policy that describes the data compliance program and that is annually certified by an officer, executive, or other employee responsible for compliance; and

- A written policy that describes the implementation of necessary security requirements and that is annually certified by an officer, executive, or other employee responsible for compliance.[10]

In addition to the newly effective requirements for U.S. Persons engaging in restricted transactions, **all U.S. Persons** are required to report prohibited transactions that they reject and that **involve data brokerage.** Specifically, any U.S. Person that has received and affirmatively rejected an offer from another person to engage in a prohibited transaction involving data brokerage on or after October 6, 2025, must report that transaction to DOJ within 14 days of the rejection. The report must include information on the rejecting entity and a detailed description of the transaction.[11]

Summary Requirements:

To achieve DSP compliance, companies **engaged in restricted transactions** should:

- Create and implement a **data compliance program** that includes risk-based procedures to understand data flows and track vendor identities.

- Develop **written policies** that outline the company's data compliance program and describe implementation of Cybersecurity and Infrastructure Security Agency (CISA) security requirements. These written policies must be **certified annually** by an officer, executive, or other employee responsible for compliance at the U.S. Entity.[12]
- Conduct and document **independent audits** that examine the company's restricted transactions, data compliance program, required records, and implementation of CISA security requirements.
- Maintain relevant records for 10 years.

Key Best Practices:

Given that the DSP regulatory requirements are now fully in effect, companies potentially subject to the DSP should consider whether their compliance programs adhere to best practices, including:

- **Understand Organizational Data Flows:** Review whether persons associated with countries of concern may have direct or indirect access to covered data. Map data flows and confirm access controls and logs are in place.
- **Evaluate Vendors, Customers, Employees, and Affiliates:** Identify relationships that may involve restricted or prohibited transactions under the DSP.
- **Implement a DSP Compliance Program:** Develop and implement appropriate policies and procedures, including aligning roles and responsibilities, to achieve initial and on-going compliance with the DSP.
- **Implement Security Measures:** U.S. Person entities engaged in restricted transactions must implement CISA-specified cybersecurity measures, which effectively operate to fully restrict access by covered persons.
- **Train Staff and Document Controls:** Ensure internal teams understand DSP obligations and can evidence proactive compliance, especially in policies and incident response protocols.
- **Review Public Disclosures:** SEC registrants should periodically revisit risk factors and cybersecurity governance disclosures in light of DSP requirements and attendant business impact.

Current Enforcement Posture:

As of this writing, DOJ has **not publicly announced any DSP-specific enforcement actions**, license denials, or advisory opinions. However, on September 24, 2025, DOJ updated its FAQ regarding the process and financial incentives for reporting possible violations of the DSP, which suggests that the rule and its enforcement remain on DOJ's radar.[13] DOJ may also begin enforcement with **non-public inquiries or informal outreach**, consistent with how other national security and export-control regimes operate. U.S. Person companies—particularly those undertaking restricted transactions or with significant data exposure to countries of concern—

would be prudent to assume that they could be asked for information or documentation related to possible restricted transactions at any time.

Self-Test for DSP Compliance:

Some preliminary questions to help guide analysis of DSP compliance, particularly with respect to the key audit, recordkeeping, and reporting obligations that recently came into effect, include:

- Do we know whether we, our vendors, or our data processors provide access to covered data to covered persons?
- For companies not engaged in restricted transactions:
    - Have we documented the procedures by which we confirmed that the company does not engage in restricted transactions or is at low risk of engaging in restricted transactions?
    - Do we have measures in place to periodically affirm that this remains the case, and to monitor for any material changes in risk profile?
    - Do we have contractual provisions for suppliers, vendors, or other third parties with access to company data prohibiting the onward transfer or resale of government-related data or bulk U.S. sensitive personal data to countries of concern or covered persons?
    - Is there a named officer or governance body accountable for DSP compliance?
- For companies engaged in restricted transactions:
    - Can we produce documentation of compliance measures, including security measures, implemented since April 8, 2025, or at least October 6, 2025?
    - Is there a named officer or governance body accountable for DSP compliance?
    - Are our audit, monitoring, and (as appropriate) reporting tools live and tested—not just drafted?
    - Can we log and trace covered transactions, access rights, and training efforts?

[1] Exec. Order No. 14117, "Preventing Access to Americans' Bulk Sensitive Personal Data and U.S. Government-Related Data by Countries of Concern," 89 Fed. Reg. 15421 (issued Feb. 28, 2024; published Mar. 1, 2024).

[2] *See* Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern, 90 Fed. Reg. 1636 (Jan. 8, 2025); Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern, 90 Fed. Reg. 16466 (Apr. 18, 2025) (codified at 28 C.F.R. §§ 202 et seq.); *see also* Dep't. of Justice, DSP Compliance Guide (Apr. 11, 2025), https://www.justice.gov/opa/media/1396356/dl; Dep't. of Justice, DSP: Frequently Asked Questions (Sept. 24, 2025), https://justice.gov/nsd/media/1415006/dl; Dep't. of Justice, DSP: Implementation and Enforcement Policy Through July 8, 2025 (Apr. 11, 2025), https://www.justice.gov/opa/media/1396346/dl?inline.

[3] Dep't. of Justice, DSP: Implementation and Enforcement Policy Through July 8, 2025, at p. 3 (Apr. 11, 2025), https://www.justice.gov/opa/media/1396346/dl?inline.

[4] Dep't. of Justice, DSP Compliance Guide (Apr. 11, 2025) at 15, https://www.justice.gov/opa/media/1396356/dl.

[5] Dep't. of Justice, DSP: Frequently Asked Questions (Sept. 24, 2025) at 35 (Question 85), https://justice.gov/nsd/media/1415006/dl.

[6] Audits for restricted transactions, 28 C.F.R. § 202.1002 (2025), https://www.ecfr.gov/current/title-28/section-202.1002.

[7] Records and recordkeeping requirements, 28 C.F.R. § 202.1101 (2025), https://www.ecfr.gov/current/title-28/section-202.1101.

[8] Records and recordkeeping requirements, 28 C.F.R. § 202.1101 (2025), https://www.ecfr.gov/current/title-28/section-202.1101.

[9] Annual reports, 28 C.F.R. § 202.1103 (2025), https://www.ecfr.gov/current/title-28/section-202.1103.

[10] Due diligence for restricted transactions, 28 C.F.R. § 202.1001 (2025), https://www.ecfr.gov/current/title-28/section-202.1001.

[11] Reports on rejected prohibited transactions, 28 C.F.R. § 202.1104 (2025), https://www.ecfr.gov/current/title-28/section-202.1104.

[12] *See* Dep't. of Justice, DSP Compliance Guide (Apr. 11, 2025) at 17, https://www.justice.gov/opa/media/1396356/dl.

[13] Dep't. of Justice, DSP: Frequently Asked Questions (Sept. 24, 2025) at 39–40 (Question 106), https://justice.gov/nsd/media/1415006/dl.

The following Gibson Dunn lawyers prepared this update: Vivek Mohan, Stephenie Gosnell Handler, Mellissa Campbell Duru, Melissa Farrar, Christine Budasoff, Hugh Danilack, and Sarah Pongrace.

Gibson Dunn lawyers are advising clients across sectors in building and validating their DSP compliance programs. We remain closely engaged with evolving guidance and agency posture and are available to assist in addressing any questions you may have about these developments and your own DSP readiness. Please contact the Gibson Dunn lawyer with whom you usually work, any of the following leaders and members of the firm's DOJ DSP Task Force or its Privacy,

Cybersecurity & Data Innovation, International Trade Advisory & Enforcement, or Securities Regulation & Corporate Governance practice groups, or the authors:

Vivek Mohan – Palo Alto (+1 650.849.5345, vmohan@gibsondunn.com)
Stephenie Gosnell Handler – Washington, D.C. (+1 202.955.8510, shandler@gibsondunn.com)
Mellissa Campbell Duru – Washington, D.C. (+1 202.955.8204, mduru@gibsondunn.com)
Melissa Farrar – Washington, D.C. (+1 202.887.3579, mfarrar@gibsondunn.com)
Christine Budasoff – Washington, D.C. (+1 202.955.8654, cbudasoff@gibsondunn.com)
Hugh N. Danilack – Washington, D.C. (+1 202.777.9536, hdanilack@gibsondunn.com)
Sarah L. Pongrace – New York (+1 212.351.3972, spongrace@gibsondunn.com)

Privacy, Cybersecurity & Data Innovation:
Ashlie Beringer – Palo Alto (+1 650.849.5327, aberinger@gibsondunn.com)
Keith Enright – Palo Alto (+1 650.849.5386, kenright@gibsondunn.com)
Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650.849.5203, cgaedt-sheckter@gibsondunn.com)
Svetlana S. Gans – Washington, D.C. (+1 202.955.8657, sgans@gibsondunn.com)
Stephenie Gosnell Handler – Washington, D.C. (+1 202.955.8510, shandler@gibsondunn.com)
Jane C. Horvath – Washington, D.C. (+1 202.955.8505, jhorvath@gibsondunn.com)
Vivek Mohan – Palo Alto (+1 650.849.5345, vmohan@gibsondunn.com)
Hugh N. Danilack – Washington, D.C. (+1 202.777.9536, hdanilack@gibsondunn.com)

International Trade Advisory & Enforcement:
Matthew S. Axelrod – Washington, D.C. (+1 202.955.8517, maxelrod@gibsondunn.com)
Adam M. Smith – Washington, D.C. (+1 202.887.3547, asmith@gibsondunn.com)
David P. Burns – Washington, D.C. (+1 202.887.3786, dburns@gibsondunn.com)
Stephenie Gosnell Handler – Washington, D.C. (+1 202.955.8510, shandler@gibsondunn.com)
Christopher T. Timura – Washington, D.C. (+1 202.887.3690, ctimura@gibsondunn.com)
Michelle A. Weinbaum – Washington, D.C. (+1 202.955.8274, mweinbaum@gibsondunn.com)
Roxana Akbari – Orange County (+1 949.475.4650, rakbari@gibsondunn.com)
Karsten Ball – Washington, D.C. (+1 202.777.9341, kball@gibsondunn.com)
Sarah L. Pongrace – New York (+1 212.351.3972, spongrace@gibsondunn.com)
Anna Searcey – Washington, D.C. (+1 202.887.3655, asearcey@gibsondunn.com)

Securities Regulation & Corporate Governance:
Aaron Briggs – San Francisco (+1 415.393.8297, abriggs@gibsondunn.com)
Mellissa Campbell Duru – Washington, D.C. (+1 202.955.8204, mduru@gibsondunn.com)
Elizabeth Ising – Washington, D.C. (+1 202.955.8287, eising@gibsondunn.com)
Thomas J. Kim – Washington, D.C. (+1 202.887.3550, tkim@gibsondunn.com)
Brian J. Lane – Washington, D.C. (+1 202.887.3646, blane@gibsondunn.com)
Julia Lapitskaya – New York (+1 212.351.2354, jlapitskaya@gibsondunn.com)
Ronald O. Mueller – Washington, D.C. (+1 202.955.8671, rmueller@gibsondunn.com)
Michael A. Titera – Orange County (+1 949.451.4365, mtitera@gibsondunn.com)
Geoffrey E. Walter – Washington, D.C. (+1 202-887-3749, gwalter@gibsondunn.com)
Lori Zyskowski – New York (+1 212.351.2309, lzyskowski@gibsondunn.com)