View on our website.

DOJ Data Security Program Task Force Update September 29, 2025

Gibson Dunn DOJ Data Security Program Task Force Update – How Are Companies Responding?

This update summarizes preliminary observations about where companies are focusing their compliance efforts, the challenges they are grappling with, and initial observations of public company disclosures involving the Data Security Program.

I. Introduction

As discussed in our previous client alert, on December 27, 2024, the Department of Justice (DOJ) issued a final rule pursuant to a mandate set out in Executive Order 14117 that established a new federal regulatory framework for "bulk sensitive personal data" and "United States government-related data."[1] This framework, which came into effect on April 8, 2025, has been referred to by DOJ as the "Data Security Program" (DSP).[2]

Despite the DSP's effective date, DOJ de-prioritized DSP civil enforcement against persons who made "good faith" efforts to comply with the DSP, for a period of 90 days. Full enforcement of the DSP began on July 9, 2025, after which DOJ made clear 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]

In the two months since July 9, and in the lead-up to the October 6, 2025 deadline by which companies engaging in restricted transactions are expected to adopt and be able to demonstrate compliance measures (including audit, reporting, and certification requirements), companies continue to assess their potential exposure under the DSP, take steps to manage and mitigate attendant risks, and build out their compliance programs. But given the challenges associated with complying with a complex—and sometimes vague, opaque, and inconsistent—rule and the lack of any enforcement history, companies are moving forward under a cloud of uncertainty.

This alert summarizes some preliminary observations about where companies are focusing their compliance efforts and challenges they are grappling with ahead of the October 6 deadline. We also discuss our initial observations of public company disclosures involving the DSP.

II. Compliance, Governance, and Risk Management Observations

In our July client alert, we recommended that companies seeking to comply with the DSP prioritize conducting a data risk assessment, implementing security measures, and building out a compliance program. While the "data compliance program" spelled out in the DOJ Compliance Guide is, in theory, only required for companies that are actually engaged in restricted transactions, companies should take steps to determine whether the DSP's prohibitions and restrictions apply to their activities. As a practical matter, for risk-reduction purposes, many companies—such as global multinationals, domestic companies engaged in global supply chain activities or with a global customer base, and even domestic companies that have offshore customer support or back-office functions—are strategically implementing many of the same programmatic elements that the DSP requires, even if they do not presently engage in restricted transactions.

Because the DSP is a novel regulatory regime, companies are creating new internal policies and processes; identifying data flows; evaluating—and, where necessary, adjusting—vendor and supplier relationships; recalibrating employee roles or responsibilities; evaluating and deploying new security measures; articulating expectations to subsidiaries, affiliates, and third parties; and revising existing contracts. The degree to which companies not engaged in restricted transactions implement each aspect of the "data compliance program" will vary based on their assessed risk exposure. However, because compliance with the DSP is not a point-in-time exercise, but rather an ongoing obligation, many companies are implementing at least a baseline framework for regularly evaluating DSP-related risks.

Since the end of the enforcement grace period in July, companies have continued to focus on the following key compliance, governance, and risk management issues:

- **Understanding Organizational Data Flows:** DOJ makes clear in the final rule and the compliance guide that companies should "know their data," including the kinds and volumes of data collected about or maintained on U.S. persons or U.S. devices, where that data is stored, who has access to it, and what it is used for. Given the proliferation of data held by companies, the disparate systems on which it is stored and used, and the increasingly global access to that data across companies, developing a clear and accurate picture of organizational data and data flows is complex and challenging. Despite the complexity, determining what data that may be subject to DSP requirements is collected, processed, stored, and transmitted by a company is a key

initial step for the company to evaluate its level of exposure to the DSP's requirements. Developing an accurate understanding of an organization's data requires sustained engagement with appropriate personnel who can speak authoritatively about the organization's data and can be a time-intensive process.

- **Identifying DSP Compliance Risk:** Once a company has developed an understanding of its data, identifying DSP compliance risk requires examining key vendors, customers, employees, and affiliates to ascertain the potential that the company may directly or indirectly provide access to bulk U.S. sensitive personal data to a covered person or country of concern. The compliance risk analysis process often raises some of the most difficult interpretive challenges under the DSP. Some key questions companies have been wrestling with include:
    - What constitutes "access" to covered data?
    - Where may access controls be considered sufficient to prevent a data transaction from qualifying as a restricted transaction altogether? Conversely, when are access controls better considered to be "security requirements" that may, if appropriately implemented, allow a company to proceed with a restricted transaction?
    - What constitutes sensitive personal data, particularly when considering hardware-based identifiers?
    - What are the boundaries of the enumerated exemptions, particularly the "corporate group transactions" exemption?
    - What is the appropriate level of diligence for a company to conduct on vendors, customers, employees, or affiliates?

- **Establishing an Organization's DSP Compliance Program:** Taken together, the DSP and DOJ's DSP Compliance Guide and Frequently Asked Questions provide a set of required and recommended actions that companies should consider when seeking to build an effective DSP compliance program.[4] Companies should implement tailored programs based on their compliance risk analyses, the nature and scope of their covered data transactions, and their respective risk tolerances. Some measures that companies are generally considering and implementing include the following:
    - reviewing, and if appropriate, supplementing existing corporate governance guidelines, charters, policies, and procedures to incorporate the DSP's core compliance requirements;
    - reviewing new and existing customer and vendor contracts, including form contracts, and considering contractual clauses designed to obtain representations of compliance with the DSP;
    - assessing auditing, reporting, and recordkeeping obligations under the DSP;
    - developing training for employees and senior leadership regarding DSP compliance obligations;
    - memorializing the company's policies and directives relating to data access by subsidiaries located outside the Unites States; and

    - documenting DSP compliance representations by non-U.S. covered and non-covered person subsidiaries, depending on the type of data involved.

- **Assigning Roles and Responsibilities for Compliance**: DOJ is clear that a strong compliance program will include the following:
    - senior management support and buy-in;
    - specific responsibilities for senior leadership;[5] and
    - a designated individual with sufficient authority, technical expertise, and resourcing to lead the development and implementation of its DSP compliance program.[6]

Companies with any level of restricted transaction risk will want to establish a strong tone from the top. As a practical matter, this will likely involve appointing an individual or committee that is accountable for oversight of work across the company (and who has the support of senior leadership) to coordinate action on the DSP's wide-ranging requirements. Such cross-company leadership and accountability is key to building a strong compliance program. However, determining DSP compliance leadership and responsibilities can present cross-organizational challenges. While elements of a DSP compliance program align with existing roles and capabilities, the DSP does not fit neatly into many companies' existing compliance structures because it implicates multiple cross-company functions and competencies, including information security, privacy, export controls/sanctions, as well as other established legal and compliance teams.

III. Public Company Disclosure Observations

Preliminary observations from a sample survey of companies' Securities and Exchange Commission (SEC) filings since the DSP's effective date of April 8, 2025 revealed limited disclosure related to the DSP.[7] Only two of the S&P 500 companies that filed a 10-K and six of the S&P 500 companies that filed a 10-Q in the five and a half months since the effective date of the regulations included a DSP-related disclosure. Of this limited data set, the majority of such disclosures appear in the Risk Factor discussion of companies' periodic reports.[8] A range of industries are represented among the companies with filings that included DSP-related disclosure, although given the small sample size, it is difficult to extrapolate broader takeaways based on the filings to date.

Against the backdrop of ongoing DSP compliance efforts and upcoming entry into effect of all portions of the regulations, DSP-related disclosures for fiscal year 2025 annual filings may become more common. Gibson Dunn's DOJ DSP Task Force will continue to monitor these trends.

[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 (Apr. 11, 2025), https://www.justice.gov/opa/media/1396351/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] *See* 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 (Apr. 11, 2025), https://www.justice.gov/opa/media/1396351/dl.

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

[6] *Id.*

[7] Filings made between April 8, 2025 and September 29, 2025 were surveyed.

[8] The effective date of the DSP came after most December 31 fiscal year-end public companies had filed their annual reports for the 2024 fiscal year. Accordingly, the number of 10-K filings in the sample survey is limited.

The following Gibson Dunn lawyers prepared this update: Vivek Mohan, Stephenie Gosnell Handler, Melissa Farrar, Mellissa Campbell Duru, Christine Bonomo, Hugh Danilack, Jill Refvem, Kyle Clendenon, and Anne Lonowski.

Gibson Dunn lawyers are available to assist in addressing any questions you may have about these developments. 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 and 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)
Melissa Farrar – Washington, D.C. (+1 202.887.3579, mfarrar@gibsondunn.com)
Mellissa Campbell Duru – Washington, D.C. (+1 202.955.8204, mduru@gibsondunn.com)
Christine Bonomo – San Francisco (+1 415.393.4627, cbonomo@gibsondunn.com)
Hugh N. Danilack – Washington, D.C. (+1 202.777.9536, hdanilack@gibsondunn.com)
Jill Refvem – Washington, D.C. (+1 202.887.3794, jrefvem@gibsondunn.com)

Kyle D. Clendenon – Houston (+1 346.718.6641, kclendenon@gibsondunn.com)
Anne Lonowski – Washington, D.C. (+1 202.777.9427, alonowski@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:

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)
James J. Moloney – Orange County (+1 949.451.4343, jmoloney@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)