Cooley

October 6 Compliance Deadline for DOJ's Data Security Program: What Companies Need to Know

October 7, 2025

The US Department of Justice's Data Security Program (DSP) has entered a critical phase. As of October 6, 2025, US persons and entities engaged in certain covered data transactions must be fully compliant with the DSP's due diligence, audit, recordkeeping and reporting requirements. With the deadline now passed, companies should assess their exposure and ensure they finalize implementation of the DSP's requirements if engaging in covered data transactions.

Refresher: What is DOJ's Data Security Program?

The DSP, which took effect in April 2025, is a federal rule designed to restrict or prohibit transactions involving access to bulk US sensitive personal data and government-related data by "countries of concern" (including China, Russia, Iran and others) or "covered persons."

The DSP distinguishes between prohibited and restricted data transactions:

- **Prohibited transactions** (e.g., data brokerage involving covered persons and covered data transactions involving human 'omic data) are outright banned under the DSP.
- **Restricted transactions** (e.g., vendor, employment or investment agreements involving covered persons) are permitted only if the US party implements a robust data compliance program and meets specific cybersecurity requirements.

For a comprehensive overview of the DSP, including definitions of covered transactions, data elements subject to the DSP and potential exemptions, please **see our overview**.

What happened on October 6?

October 6 was the deadline for US persons or entities engaged in **restricted transactions** to comply with the DSP's due diligence, audit, recordkeeping and reporting requirements.

1. Due diligence and data compliance program

The DSP requires US persons and entities to conduct reasonable diligence before entering into restricted transactions.

Part of that ongoing diligence is captured by a written data compliance program. US persons or entities engaged in a restricted transaction must have in place this written data compliance program, that among other things, contains:

- Risk-based procedures to verify data flows, transaction parties and end uses of the bulk US sensitive data or government-related data by the counterparty.
  - The data compliance program should enable the US person or entity to identify for each restricted transaction:
    - The types and volumes of bulk US sensitive personal data or government-related data involved in a restricted transaction.

- The identity of the parties to the restricted transaction, including any ownership of entities or citizenship or primary residence of counterparties.
- The end use of the data by the counterparty and the method of data transfer to the counterparty.

- Procedures to enable the US person or entity to verify the identity of its vendors.

The US person or entity must also have in place a written policy describing the data compliance program, which must be annually certified by an officer or executive of the company.

2. Annual independent audit

US persons and entities engaged in covered data transactions as of October 6 must conduct an independent audit once per calendar year in which the US person or entity is engaging in a restricted transaction. The audit must:

- Be completed by a person who is qualified and competent to examine the company's compliance with the DSP and the security requirements. Notably, the annual audit does not need to be conducted or verified by a third party, but the auditor must be independent and cannot be a covered person or country of concern. In practice, companies may find it preferable to engage a third-party expert to conduct these audits.
- Review and evaluate:
  - The prior year's restricted transactions.
  - The data compliance program.
  - Records required to be kept under the DSP.
  - Cybersecurity and Infrastructure Security Agency (CISA) security requirements.
- Be memorialized in a written audit report, which must be submitted to the US person or entity within 60 days of completion. The report must include:
  - A description of any restricted transactions.
  - The methodology used to evaluate the compliance program and description of materials reviewed or interviews conducted.
  - A description of the effectiveness of the data compliance program and security controls.
  - A description of any vulnerabilities or security deficiencies that could create risk of access to bulk US sensitive personal data or government-related data.
  - Instances of failures of security controls or mitigation controls.
  - Recommendations to enhance compliance with the DSP's security requirements.

3. Recordkeeping

Starting October 6, 2025, US persons and entities must maintain full records of any restricted transactions for at least 10 years, including the types and volume of data involved, the dates of the transaction, the method of data transfer and other details of the transaction, as well as any annual audit reports. These records must be kept in a format that could be produced for the DOJ if requested.

4. Cloud computing-related annual reporting

US persons or entities that are owned 25% or more by a "country of concern" must file an annual report to the DOJ detailing any covered data transactions involving cloud computing services they have entered into on or after October 6, 2025. The report must cover transactions as of December 31 of the preceding year and be filed by March 1 of the subsequent year. Reports must include a description of the transaction, types and volume of data involved in the transaction, method of data transfer, and the names and

locations of any other persons participating in the transaction.

For this first year of compliance, that means any US person owned 25% or more by a “country of concern” and engaging in cloud computing-related covered data transactions will have to report those transactions between October 6 and December 31, 2025, to the DOJ by March 1, 2026.

5. **Reporting rejected transactions**

Beginning October 6, 2025, any US person or entity who rejects entering into a prohibited transaction (e.g., a data brokerage with a covered person) must report it to the DOJ within 14 days.

What should companies do now?

US persons or entities engaged in a covered data transaction should:

- **Map data flows** to identify potential exposure to countries of concern or covered persons in existing contracts and engagements that may be up for renewal or renegotiation after October 6.
- **Conduct a gap assessment** to determine what steps need to be taken to comply with the DSP’s requirements.
- **Implement or update compliance programs** to meet the DSP and CISA requirements.
- **Consider engaging a third party** to assess compliance programs and/or conduct an independent audit.
- **Prepare audit and reporting infrastructure** to meet ongoing obligations within mandated timeframes.

Need help?

Cooley’s cyber/data/privacy team is advising clients across industries on how to navigate the DOJ’s DSP. If you have questions about whether your transactions are covered or how to implement a compliant DSP program, please reach out.

Key Contacts

Michael Egan Washington, DC	megan@cooley.com +1 202 776 2249

Mari Dugas Washington, DC	mdugas@cooley.com +1 202 740 0747
Emma Plankey Boston	eplankey@cooley.com +1 617 937 1349