Stay Current

PAUL HASTINGS

July 2026

Follow us on LinkedIn

PH Privacy

The Approaching Audit and Certification Deadlines Under the Bulk Data Transfer Rule

By Aaron Charfoos, Michelle A. Reed, Rachel Kurzweil and Alan Huang

The U.S. Department of Justice's Bulk Data Transfer Rule sets out a significant new data governance requirement for companies across a wide range of sizes and industries. We previously wrote on the rule in the following posts: DOJ and CISA Issue Final Rules Regulating Export of Bulk Sensitive Data and Department of Justice Provides New Guidance on Bulk Sensitive Data Transfer Rules. In this alert, we want to focus on two upcoming deadlines that companies should prepare for — the audit and certification requirements.

Specifically, in 2025, the DOJ established the Data Security Program (DSP) under a Final Rule implementing Executive Order 14117 (Final Rule), and concurrently, the U.S. Department of Homeland Security's Cybersecurity Infrastructure Security Agency (CISA) issued security requirements for companies engaging in restricted transactions (CISA Security Requirements). The DSP, which has been fully in effect since October 2025, restricts or prohibits transactions that would give countries of concern access to bulk U.S. sensitive personal data or government-related data. To assist companies with compliance, the DOJ's National Security Division (NSD) published three guidance documents to aid in complying with the Final Rule: a Compliance Guide, a Frequently Asked Questions page and an Implementation and Enforcement Policy.

The DSP sets specific reporting requirements for entities engaging in restricted transactions and also has an annual audit and recertification requirement, as detailed below.

Annual Audit

Companies engaging in restricted transactions are also required to maintain a written data compliance program (DCP) — a written policy that implements the CISA Security Requirements and maintains specific records documenting its due diligence processes. These documents must be certified annually by a responsible officer, executive or employee responsible for compliance. Additionally, companies engaging in restricted transactions must conduct an annual independent audit of their restricted transactions, DCP, CISA Security Requirement policy and recordkeeping. As the audit requirements for the Final Rule took effect Oct. 6, 2025, both the annual certification and audit should be completed by October 2026.

Among many requirements, key aspects of the audit include:

- **Scope**: The audit must comprehensively examine the restricted transactions, the data compliance program and its implementation, the records required under the Final Rule and the applicable CISA security controls.
- **Independence**. The auditor may not be a covered person or affiliated with a country of concern, and the DOJ frames the required independence as being objective, fact-based, nonpartisan and nonideological with respect to both the company and the transactions under review. The DOJ permits internal auditors but cautions that internal audits often lack the independence of an external review.
- **Use of Existing Audits**. The Final Rule mandates no standalone audit or particular auditing standard. An audit conducted for another purpose can satisfy the requirement as long as it expressly addresses the DSP's requirements and follows a reliable methodology.
- **Written Report**. The audit must be memorialized in a written report delivered to the company within 60 days of completion, describing the restricted transactions, the methodology and materials reviewed, the effectiveness of the compliance program and security controls, any vulnerabilities or control failures and recommendations to strengthen compliance.
- **Retention**. The report, the documentation of each restricted transaction, and the related due diligence must be retained for at least 10 years in a form producible to the DOJ on request.

Certification of Compliance

In addition to the audit, companies must also annually certify: (1) the company's Data Compliance Program implementation and due diligence efforts; (2) the company's implementation of the CISA Security Requirements; and (3) the completeness and accuracy of recordkeeping documenting the company's due diligence. This annual certification must be retained and furnished to the DOJ upon request. Notably, in the DOJ's Compliance Guide, the audit is meant to support the annual certification. Specifically, companies must certify. The DOJ also notes that this "certification process is an opportunity for senior management to reassess the Data Compliance Program and report conclusions about the effectiveness of the company's internal controls," and it recommends that the senior personnel also certify:

- Whether the company has processes in place to establish, maintain, review, test and modify its written policies and procedures, that are reasonably designed to achieve compliance with the DSP.
- That the attestation is evidenced in a report that has been reviewed by the chief executive officer and that a final report has been submitted to the company's board of directors and audit committee.
- Whether there are changes in internal controls or factors impacting internal controls subsequent to the date of the report's evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses.
- That, based on the officer's knowledge, the report does not contain any untrue statement of material facts and does not omit any material facts.
- Whether compliance personnel have conducted one or more meetings with the chief executive officer(s) in the preceding 12 months to discuss compliance with the DSP; or
- The chief executive officer has consulted with the chief compliance officer(s), other officers as applicable, and other employees, outside consultants, lawyers, auditors and accountants, to the extent deemed appropriate, in order to verify the statements made in this certification.

Based on the DOJ's guidance, it is clear that the certification is a substantive attestation rather than a procedural formality as the certifying officer must represent that the program performs as the Final Rule requires — verifying data flows, identifying the transacting parties and their ownership, confirming the end use and method of transfer, and authenticating vendor identities. Because the attestation is only as sound as the program beneath it, a company should consult with experts and test their programs before the anniversary rather than presume their sufficiency.

Other Reporting Requirements

It is also worth remembering that the DSP requires that U.S. persons who are engaged in restricted transactions involving cloud-computing services and have 20% or more equity interests owned (directly or indirectly, through any contract, arrangement, understanding, relationship or otherwise) by a country of concern or covered person annually report such transactions to the NSD. The first report was due March 1, 2026.

The DSP also requires that U.S. persons report any known or suspected violations of onward disclosure limitations of bulk U.S. sensitive personal data or government-related data by foreign persons.

The Paul Hastings Data Privacy and Cybersecurity and Global Trade Controls practices regularly advise on related matters and are closely monitoring developments related to the Final Rule. If you have any questions concerning how the Final Rule may affect your organization, please do not hesitate to contact any member of our team.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Chicago

Aaron Charfoos
+1-312-499-6016
aaroncharfoos@paulhastings.com

Dallas

Michelle A. Reed
+1-972-936-7475
michellereed@paulhastings.com

Washington, D.C.

Rachel Kurzweil
+1-202-551-1940
rachelkurzweil@paulhastings.com

Alan Huang
+1-202-551-1765
alanhuang@paulhastings.com