VENABLE LLP

A Closer Look at the Data Security Requirements in DOJ's Bulk Data Rule

June 03, 2025

Jennifer Daskal, Kelly DeMarchis Bastide and Caitlin Clarke

As described in an earlier alert, the Department of Justice (DOJ) recently announced a 90-day pause in enforcement of the "Bulk Data Rule" for entities engaging in good faith compliance. That 90-day grace period ends on July 8, 2025—a date that is fast approaching. While certain auditing, due diligence, and reporting obligations do not go into effect on October 6, companies are expected to comply with all other aspects of the DOJ Bulk Data Rule by the end of the grace period.

As also detailed in earlier alerts, the Bulk Data Rule *prohibits* certain transactions—namely those that involve the sale or transfer of bulk U.S. sensitive data or government data to a "country of concern" (currently China, Cuba, Iran, North Korea, Russia, and Venezuela) or "covered person." A covered person includes, but is not limited to, an entity that is organized or chartered in a country of concern; is an employee, contractor, or resident of a county of concern; or is 50% or more owned, individually or in the aggregate, by one or more countries of concern or covered persons of concern.

The rule *restricts* other transactions—namely those that include vendor, employment, or investment agreements that involve access to bulk U.S. sensitive data or government data to a country of concern or covered person. Restricted transactions are permitted if they comply with the security requirements promulgated by the Cybersecurity and Infrastructure Security Agency (CISA), along with the other applicable due diligence, auditing, and reporting obligations.

Without putting into place the CISA security requirements, such transactions are prohibited. (That said, *all* covered data transactions that involve access to bulk human genomic data or human biospecimens from which such data can be derived are prohibited, even if the transaction includes a vendor, employment, or investment agreement.)

In this alert, we provide general information about how to comply with the security requirements for the *subset* of restricted transactions that are subject to the rule.

CISA Security Requirements for Bulk Data Rule Compliance

At a broad level, the CISA Security Requirements are designed to mitigate the risk of sharing U.S.-government-related and bulk U.S. sensitive data with countries of concern or covered persons.

They include two categories of requirements: on the organization and system as a whole, and on the

specific data that is included in a restricted transaction. While the organizational and system-level requirements are mandated for any U.S. company engaged in restricted transactions, companies have some flexibility in determining what data-level requirements sufficiently address the risks posed.

Organizational and System-Level Requirements

Most of the organizational and system-level requirements track what is already recommended by the National Institute of Standards and Technology (NIST) Cybersecurity and Privacy Framework, as well as other already-in-place CISA-issued Cross-Sector Cybersecurity and Performance Goals.

They include requirements to

- Identify, prioritize, and document all assets of a covered system
- Designate an individual to be accountable for cybersecurity and compliance functions
- Document all vendor and supplier agreements
- Develop and implement incident response plans
- Implement access controls to prevent covered persons or countries of concern from gaining access to covered data that does not comply with the data-level requirements
- Conduct an internal risk assessment, which in turn is intended to guide implementation of the data-level requirements

The organizational and system-level requirements also include an obligation to remediate all known exploited vulnerabilities, starting with the most critical assets first, and completing all vulnerability remediation within 45 calendar days.

Data-Level Requirements

The data-level requirements are less prescriptive. Instead, they require companies to implement a "combination" of the identified mitigations, so as to prevent countries of concern and covered persons from gaining access to bulk U.S. personal data and government-related data, in accordance with the mandated organizational-level risk assessment.

The list of mitigations includes

- The application of data minimization and data making strategies
- Use of comprehensive encryption techniques
- Application of privacy-enhancing techniques
- Implementation of identity and access management techniques to deny authorized access to covered data by covered persons or countries of concern

Here, too, the NIST Privacy Framework provides useful guidance as to how to effectively implement these mitigation measures.

Additional DOJ Compliance Requirements

Beginning on October 6, 2025, U.S. companies will also be required to have in place a written data compliance program that is annually certified by a company officer, executive, or other employee responsible for compliance; conduct annual audits of restricted transactions; and keep specified records regarding restricted transactions.[1]

For a more detailed assessment of how these security requirements may apply to your organization, as well as specific guidance on compliance, please contact the authors or visit Venable's Privacy and Data Security web page. And be sure to check out Venable's Data Breach Notification Law Handbook.

---

[1] See 28 C.F.R. §§ 202.1001, 202.1002, 202.1103, 202.1104.