BAKER BOTTS

PARTNER TO THE INNOVATORS

America's Data Firewall: Understanding DOJ's Final Rule on Sensitive Personal Data Transfers

Matthew Baker

Practice Chair – Privacy & Cybersecurity

Jenna Comizio

Vice President, Compliance & Legal Affairs

Background

The U.S. Department of Justice (DOJ) issued a final rule ("the Rule") under Executive Order 14117, aimed at preventing access to Americans' bulk sensitive personal data and government-related data by designated "countries of concern" and associated "covered persons."

This rule took is in full effect as of October 6, 2025, and the Trump administration has prioritized the DSP, describing it as consistent with the administration’s “America First Investment Policy”.

Significance

The DOJ created the DSP to establish rules for U.S. persons and entities engaging in certain data transactions that the U.S. Government has determined pose an unacceptable risk of giving “countries of concern” or “covered persons” access to government-related data or bulk U.S. sensitive personal data.

Among other requirements, the DSP identifies classes of prohibited and restricted transactions, identifies countries of concern and classes of covered persons to whom the proposed rule applies, identifies classes of exempt transactions, and establishes processes to issue licenses authorizing certain prohibited or restricted transactions.

Impacts organizations that store, process, broker, or facilitate access to bulk U.S. sensitive personal data or government-related data.

Key Terms under the Rule

Term	Meaning
Countries of Concern	China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba, Venezuela
Covered Persons	Entities or individuals that meet any of the following: 1) Organized or headquartered in a country of concern; 2) 50%+ owned (directly or indirectly) by such countries or nationals; 3) Employed or contracted by a country of concern; 4) Primarily residing in a country of concern; or 5) Designated by the Attorney General as acting for or being controlled by a country of concern.
Sensitive Personal Data	Precise geolocation, biometrics, ‘omic, health, and financial data
Government-Related Data	Information about U.S. federal employees, contractors, military, etc.
Prohibited Transactions	E.g., sale of U.S. Sensitive Personal Data to Covered Persons or Country of Concern, transfer of human ‘omic data to China
Restricted Transactions	An employment, vendor, or investment transactions that permits a Covered Person or Country of Concern access to U.S. Sensitive Personal Data; permitted only if in compliance with the Rule and in compliance with CISA-specified security requirements.
Exempt Transactions	E.g., official U.S. government business, academic research
Access	Logical or physical access, including the ability to obtain, read, copy, decrypt, edit, divert, release, affect, alter the state of, or otherwise view or receive, in any form, including through information systems, information technology systems, cloud-computing platforms, networks, security systems, equipment, or software.

U.S. Sensitive Personal Data Bulk Thresholds

Data Type	Description	Bulk Threshold
Human 'omic data	Genomic, epigenomic, proteomic, transcriptomic	>1,000 (or 100 for genomic)
Biometric identifiers	Fingerprints, voice, retina scans, etc.	>1,000 persons
Precise geolocation	Within 1,000 meters	>1,000 devices
Personal health data	Diagnoses, treatments, meds, physical metrics	>10,000 persons
Personal financial data	Banking, credit, trading data	>10,000 persons
Covered personal identifiers	Combinations defined identifiers linked to an individual	>100,000 persons
Government-Related Data	Geolocation around sensitive U.S. areas; data on current/former U.S. government personnel	No bulk threshold

Significance

Covered Personal Identifiers: Any two or more of the following: full or truncated government identification or account number; (2) full financial account numbers; (3) device-based identifier (MAC, SIM); (4) demographic or contact data; (5) advertising identifier (Apple ID for Advertisers, Google Advertising ID); (6) account-authentication data; (7) Network-based identifier (IP address); or (8) call-detail data (CPNI).

Bulk: Any amount of sensitive personal data that meets or exceeds the thresholds, whether through a single transaction or aggregated across transactions involving the same U.S. person.

Access: Broadly defined and includes even theoretical access.

Bulk Sensitive Personal Data: Format neutral and regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted.

“Know Your Data” Requirements

Entities subject to the DSP must develop and implement “know your data” compliance programs to verify data transactions, including:

- the nature and volume of data;
- how the data is used;
- and how the data is marketed.

DOJ guidance clarifies that entities are not expected to decrypt or aggregate data in their possession to comply with the Rule’s "know your data" standard. This explanation is aligned with the DSP final rule’s explanation that cloud service providers will not be expected to “know” their customers’ encrypted data to comply with DSP.

Prohibited Transactions

These transfers are strictly banned :

- Data Brokerage with Covered Persons / Countries of Concern
- Access to bulk Human ‘Omic Personal Data or biospecimens by Covered Persons or Countries of Concern
- Transactions violating restricted transfer requirements laid down by the Rule, *e.g.*, without required CISA security controls

Knowingly directing a prohibited transaction is, likewise, prohibited.

Examples of Prohibited Transactions

Data Brokerage Transactions: A U.S. data broker sells a database of 1.2 million Americans' health records (names, dates of birth, insurance info) to a Chinese marketing firm.

Government-Related Data Transfers: A U.S. real estate data company sells geolocation data that incidentally includes detailed mapping of military base housing locations to an Iranian-owned mapping company.

Onward Transfers Without Safeguards: A U.S. fitness app sells user workout data to a British analytics firm without any contract limiting further resale. That firm later resells the data to a Hong Kong health tech company.

Restricted Transfers

Permissible only if compliant with the Rule and CISA Security Requirements:

- **Vendor Agreements**: Contracts for services (e.g., cloud hosting, data processing)
- **Employment Agreements**: Hiring individuals residing in or affiliated with countries of concern
- **Investment Agreements**: Acquiring control or ownership in U.S. entities or real estate (excluding passive holdings)

Examples of Restricted Transfers

Vendor Agreement: A U.S. telehealth platform enters into a cloud services agreement with a Russian-owned vendor to store bulk personal health data from over 10,000 users.

Employment Agreement: A U.S. company sells goods and collects bulk personal financial data about its U.S. customers. The U.S. company appoints a citizen of a country of concern, who is located in a country of concern, to its board of directors. This director would be a covered person, and the arrangement appointing the director would be an employment agreement. In connection with the board's data security and cybersecurity responsibilities, the director could access the bulk personal financial data. The director's employment would be a restricted transaction.

Investment Agreement: A U.S. company intends to build a data center located in a U.S. territory. The data center will store bulk personal health data on U.S. persons. A foreign private equity fund located in a country of concern agrees to provide capital for the construction of the data center in exchange for acquiring a majority ownership stake in the data center. The agreement that gives the private equity fund a stake in the data center is an investment agreement. The investment agreement is a restricted transaction.

Exemptions to the Rule

Exemption Category	Description	Conditions
Regulatory Approval Data	Transfers of de-identified or pseudonymized data necessary for obtaining or maintaining regulatory approval to research or market a drug, biological product, device, or combination product.	Data must be de-identified or pseudonymized consistent with FDA regulations and reasonably necessary to evaluate the safety and effectiveness of the product.
Personal Communications	Transfers involving personal communications that do not involve the transfer of bulk sensitive personal data or government-related data.	Must not involve the transfer of covered data as defined by the Rule.
Financial Services Transactions	Transactions necessary for the conduct of financial services, including payment processing and anti-money laundering activities.	Must be consistent with applicable laws and regulations governing financial services.
Corporate Group Transactions	Transfers within a corporate group, such as between parent and subsidiary companies.	Transfers must not involve countries of concern and must comply with internal data protection policies.
Transactions Authorized by Federal Law or International Agreements	Transfers required or authorized by U.S. federal law or international agreements to which the U.S. is a party.	Must be explicitly authorized by the relevant legal instrument.
Investment Agreements Subject to CFIUS Action	Investment transactions that have been reviewed and are subject to action by the Committee on Foreign Investment in the United States (CFIUS).	Must be under active CFIUS review or subject to CFIUS mitigation measures.
Telecommunication Services	Transfers necessary for the provision of telecommunications services.	Must not involve the transfer of covered data to countries of concern.
Clinical Investigations	Transfers of data for clinical investigations necessary for regulatory approval.	Data must be de-identified or pseudonymized and reasonably necessary for the investigation.

Exemption: Corporate Group Transaction

Corporate Group Transaction applies when the transactions are ordinarily incident to and part of administrative or ancillary business operations, including:

Human-resources purposes;
Payroll transactions;
Paying business taxes;
Purchasing business permits or licenses;
Sharing data with auditors and law firms for regulatory compliance;
Risk management;
Business-related travel;
Customer support;
Employee benefits; or
Employee internal and external communications.

However, the exemption is narrow, contextually-driven, and does not apply to core business activities or, service provider support, such as suppliers or third-party vendors.

Diligence Requirements

Restricted Transactions must comply with:

- Written data compliance policy;
  - Risk-based procedures for verifying data flows;
  - Vendor management and validation;
  - Written security policy.
- Identity & ownership verification protocols;
- Data transfer logs (type, volume, source/destination);
- Annual officer certification of compliance; and

Audit Requirements

Restricted Transactions must comply with :

- Description of all Restricted Transactions;
- Audit methodology and results;
- Security control effectiveness and failures; and
- Recommendations for improved compliance.

Audits can be internal or external provided they are sufficiently independent.

Audits for other purposes may satisfy DSP requirements if they "specifically, sufficiently, and expressly address" DSP requirements.

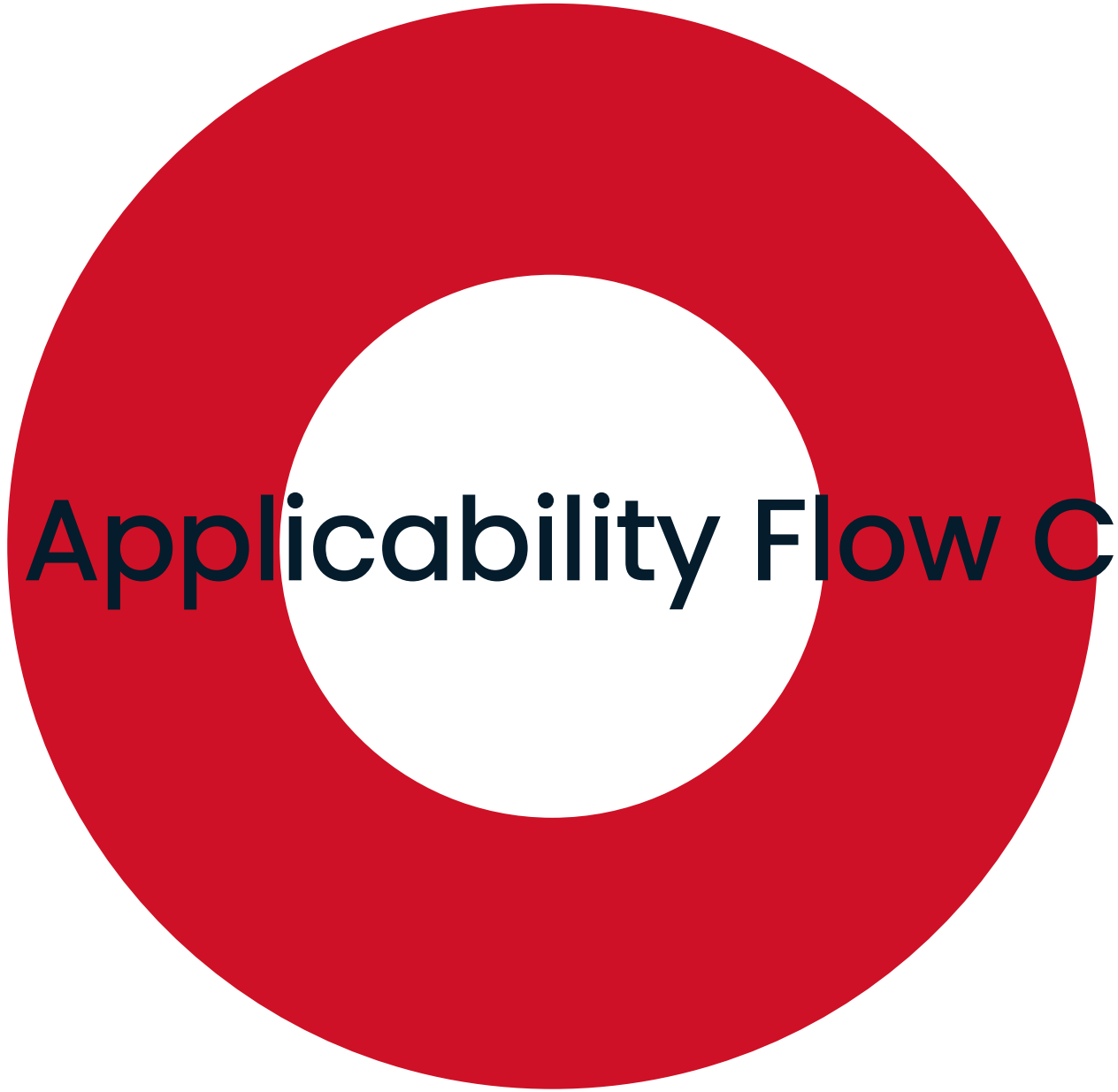
Restricted Transactions must comply with CISA's Security Requirements by October 6, 2025:

Security Capability	Description	NIST CSF Categories
Access Control	Implement role-based access controls and enforce least privilege principles to restrict data access.	PR.AC-1 to PR.AC-6
Data Protection	Encrypt sensitive data at rest and in transit; implement data loss prevention mechanisms.	PR.DS-1 to PR.DS-5
Audit and Accountability	Maintain audit logs of data access and modifications; regularly review logs for unauthorized activities.	DE.AE-1 to DE.AE-5
Incident Response	Develop and test incident response plans to address potential data breaches or security incidents.	RS.RP-1 to RS.RP-5
Continuous Monitoring	Monitor systems continuously for security events; employ intrusion detection systems.	DE.CM-1 to DE.CM-8
Configuration Management	Establish baseline configurations and manage changes to system settings to prevent unauthorized alterations.	PR.IP-1 to PR.IP-12
Supply Chain Risk Management	Assess and manage risks associated with third-party service providers and vendors.	ID.SC-1 to ID.SC-5
Training and Awareness	Conduct regular training for employees on data protection policies and procedures.	PR.AT-1 to PR.AT-5

Penalties

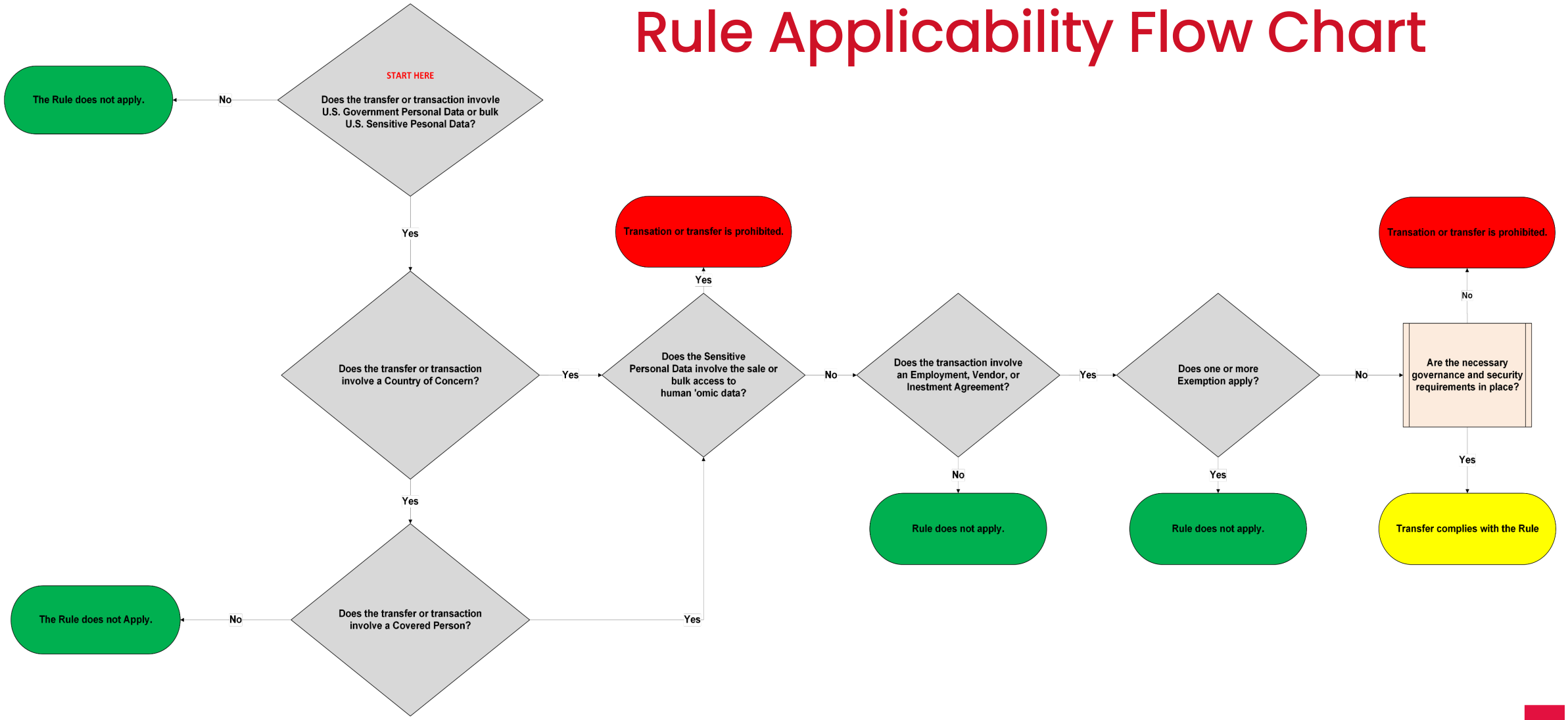
Civil	Greater of $368,136 or 2X transaction value per violation
Criminal	Up to $1 million and/or 20 years imprisonment (willful violations)

DSP incorporates a "knowing" standard, meaning DOJ will evaluate what a person "had actual knowledge of, or reasonably should have known".



Rule Applicability Flow Chart

Rule Applicability Flow Chart



This material is provided for general informational purposes only and does not constitute legal advice.

BAKER BOTTS
PARTNER TO THE INNOVATORS


Compliance
Strategies

Data Mapping

Goal: Know exactly what data you hold, and where it flows.

- **Inventory Covered Data**: Catalog all types of sensitive and government-related data handled by the organization. Pay close attention to human any government or ‘omic data.
- **Map Data Flows**: Document where data is stored, processed, and transferred — especially across borders. Identify endpoints where foreign access might occur, especially for Countries of Concern.
- **Apply Bulk Thresholds**: Use the thresholds in the Rule to flag datasets that could qualify as “bulk data” (e.g., 1,000+ individuals for biometric data).

Transaction Review

Goal: Determine whether the business is engaged in a Prohibited or Restricted transaction.

- **Identify Foreign Counterparties**: Screen counterparties to assess whether they qualify as Covered Persons or Countries of Concern.
- **Classify Transactions**: Sort relationships into the three Rule categories:
  - **Prohibited** (e.g., data brokerage with a Chinese entity)
  - **Restricted** (e.g., cloud vendor agreement with a Russian firm)
  - **Exempt** (e.g., financial services transactions)
- **Check for Downstream Risks**: Assess whether indirect exposure exists — such as a U.S.-based contractor that subcontracts to a Covered Person.

Transaction Review—A Deeper Dive

Prioritize by Risk Profile

- Start with transactions involving the largest volumes of sensitive personal or government-related data.
- Focus first on transactions involving vendors, partners, or acquirers with connections to a Country of Concern.

Implement a Vendor and Counterparty Screening Process

- Use third-party diligence tools or questionnaires to screen existing and prospective vendors and partners for connections to Countries of Concern.
- Include requirements for disclosure of beneficial ownership and control relationships.
- Build a checklist or flagging mechanism tied to onboarding processes for new vendors, M&A targets, and technology partners.

Focus on High-Risk Transaction Types

- Mergers, acquisitions, or investments involving U.S. companies with significant sensitive data.
- Data storage, analytics, cloud hosting, AI services, and telecommunications-related service agreements.
- Employment agreements involving remote work access to sensitive systems from high-risk jurisdictions.

Establish an Escalation and Legal Review Process

- Create a clear internal process to escalate potential covered transactions to legal and compliance teams for further review and mitigation planning.

CISA Security Requirements

Goal: Achieve full alignment with the CISA Security Requirements.

- **Gap Analysis**: Benchmark current cybersecurity controls against CISA's final security requirements (identity management, encryption, privacy-enhancing tech, etc.).
- **Remediate Gaps**: Implement necessary upgrades such as MFA, robust access logging, risk assessment procedures, and organizational governance.
- **Integrate into Vendor Contracts**: Include contractual commitments that prohibit resale/data brokerage and mandate reporting of violations.

Governance

Goal: Operationalize compliance at the organizational level.

- **Designate a Compliance Lead**: Appoint a responsible executive (e.g., CISO or General Counsel) to oversee Rule compliance.
- **Establish a Data Compliance Program**: Create internal SOPs for identifying, classifying, and handling covered transactions.
- **Implement Restricted Transaction Protocols**: Define approval processes, vetting checklists, and escalation channels.
- **Train Staff**: Provide ongoing training to employees in legal, procurement, IT, and vendor management roles.

Auditing

Goal: Maintain defensible records and prepare for inspections.

- **Develop and Certify Compliance Policies**: Write clear policies addressing covered data handling, foreign engagement protocols, and CISA controls. Certify annually.
- **Maintain Audit Trail**: Record all Restricted transactions, including purpose, parties, data types, and protective measures.
- **Schedule Annual Independent Audit**: Conduct and retain an audit of the data compliance program. Include findings on vulnerabilities, control failures, and recommendations.
- **Prepare for DOJ Inquiry**: Have documentation ready to respond to licensing requests, pre-penalty notices, or advisory opinion inquiries.

AUSTIN
BRUSSELS
DALLAS
DUBAI
HOUSTON
LONDON
NEW YORK
PALO ALTO
RIYADH
SAN FRANCISCO
SINGAPORE
WASHINGTON

bakerbotts.com