DOJ BULK DATA TRANSFER RULE	SOP 11.1.05

1. PURPOSE & POLICY

The purpose of this SOP is to establish institutional requirements and procedures to ensure compliance with the US Department of Justice (DOJ) Bulk Data Transfer Rule (28 CFR 202), issued under Executive Order 14117, which regulates access to and transfer of certain US sensitive personal data and government-related data to foreign persons.

2. GENERAL INFORMATION

The DOJ Bulk Data Rule prohibits or restricts US entities from transferring or allowing bulk transfers of US-related sensitive or government data to certain individuals, entities, or Countries of Concern. All data custodians, including Faculty and research personnel, are responsible for ensuring that any transfer, sharing or access to covered data complies with applicable DOJ requirements. Individuals must also evaluate whether datasets meet DOJ-defined bulk thresholds. If thresholds are met or may be met through aggregation over time, the data must be treated as covered bulk data and handled in accordance with this SOP.

Definitions:

Countries of Concern: Countries designated by the US government as posing national security risks for data access. These currently include:

- China (including Hong Kong and Macau)
- Russia
- Iran
- North Korea
- Cuba
- Venezuela

Covered Person: An individual or entity that meets one or more of the following:

- A foreign individual primarily resident in a Country of Concern
- An entity organized under the laws of, or headquartered in, a Country of Concern
- An entity owned 50% or more (directly or indirectly) by one or more Countries of Concern or their nationals
- Employees, contractors or agents of the above
- Any individual or entity specifically designated by the US Attorney General

Foreign Person: Any individual or entity that is not a US Person (i.e., is not physically located in the US)

US Person: An individual that meets one or more of the following:

- US citizens or nationals
- Lawful permanent residents (green card holders)
- Individuals physically located in the United States
- Entities organized under US law (including foreign branches)

Covered Data: Data regulated under the DOJ rule, including:

1. Sensitive Personal Data (in bulk quantities)
   - Personal Identifiers (e.g., SSN, passport numbers)
   - Financial Information
   - Health or Medical Data
   - Biometric Identifiers
   - Genomic Data
   - Precise Geolocation Data
2. Government-Related Data
   - Data linked to US government personnel or contractors
   - Data related to sensitive government locations or operations

Bulk Data: Data that meets or exceeds DOJ-defined volume thresholds for sensitivity categories within a 12-month period. If a dataset meets or exceeds any threshold below, the Bulk Data Rule's prohibitions and restrictions on data transactions apply regardless of whether the data is de-identified, anonymized, pseudonymized, or encrypted.

Type of Data	Thresholds
Covered personal identifiers of US persons	>100,000
Personal financial data of US persons	>10,000
Personal health data of US persons	>10,000
Precise geolocation data, biometric identifiers, human 'omic data (other than human genomic data) of US persons and/or devices	>1,000
Human genomic data of US persons	>100
Combination of the data detailed above	Lowest threshold of data type applies
U.S. Government related data	Any amount of data

Covered Data Transaction: Any transaction that involves access by a Country of Concern or Covered Person to any bulk US sensitive personal data or government-related data and that involves:

- Data brokerage
- Vendor agreements
- Employee agreements
- Investment or partnership agreements

Payment or other valuable consideration is an element of covered data transactions, thus research funding, gifts, revenue contracts and payment for goods or services all qualify as consideration. The Bulk Data Rule includes Exempt transactions which allow data transactions that would otherwise be prohibited or restricted. Some exemptions, however, may trigger reporting requirements.

Prohibited Transactions: Any transaction that is prohibited or requires mitigation under the DOJ Bulk Data Rule, including:

- Data brokerages with Countries of Concern or Covered Persons
- Data transactions with Countries of Concern or Covered Persons that involves access to human 'omic data (collected or maintained on more than 1,000 US Persons) or access to human biospecimens from which bulk human 'omic data could be derived.
- Data sharing with a Foreign Person who is not a Covered Person that involves the sale or licensing of bulk US sensitive personal data unless the agreement contains certain contractual prohibitions on sharing such data with a Country of Concern or Covered Persons.
- Any known or suspected violations must be reported to the DOJ within 14 days.

Restricted Transactions:

- Vendor agreements, employee agreements and investment agreements are restricted transactions subject to certain reporting, recordkeeping, data security and auditing requirements (Subpart J 202.1103, 202.1104)
- Before proceeding with any restricted transaction, the transacting party must implement a Data Security Program that includes:

    1. A data compliance program with policies and procedures for conducting risk-based reviews and annual certification
    2. Cybersecurity and Infrastructure Security Agency (CISA) Security Requirements with access controls, risk assessments, and data-level controls; and continuing audit, reporting and recordkeeping requirements.

Activities that are Not Restricted by the DOJ Bulk Data Rule:

- Domestic sharing between US Persons or entities within the US except to the extent that a US Person has not been specifically designated as a Covered Person,
- Data sharing that is without any kind of financial benefit or consideration,
- Data about non-US Persons, or
- Data sharing that is directed or authorized pursuant to the terms of a federal grant. Non-federally funded research data is not exempt.

3. TRAINING

Other than the normally required and study specific training for all human subjects research, there are no additional specific training requirements associated with the DOJ Bulk Data Transfer Rule; however, investigators should carefully read and follow this guidance.

4. PROCEDURES

A. IRB Submission

1. Any individual intending to collect, access, use, share or transfer human data or biospecimens must submit either a Query or Full Application via the IRB Protocol Application System (PAS) prior to initiating the activity.

2. The submission must include sufficient detail to enable review of the type and scope of data involved and all participating individuals and entities.

3. Activities may not proceed until the application has been reviewed and any required approvals or conditions have been issued by the IRB.

B. Screening for Foreign Involvement

As part of the protocol submission, investigators must:

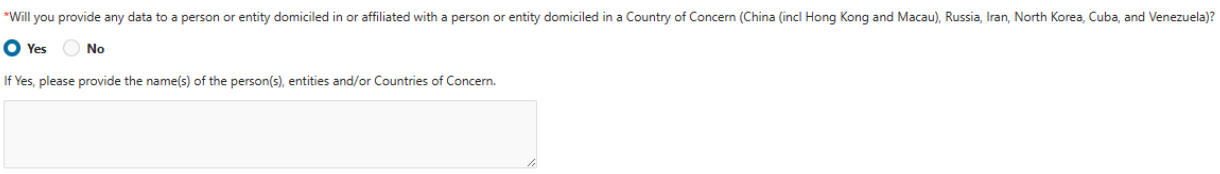
1. Identify all parties involved in the activity, including individuals, collaborators, institutions and third parties.

2. Determine whether any party is a

   a. Foreign Person,

   b. Covered Person or

   c. Located in or affiliated with a Country of Concern.



C. Identification of Covered Data

Also, as part of the protocol submission, investigators must determine whether the data involved qualifies as:

1. sensitive personal data (bulk) or

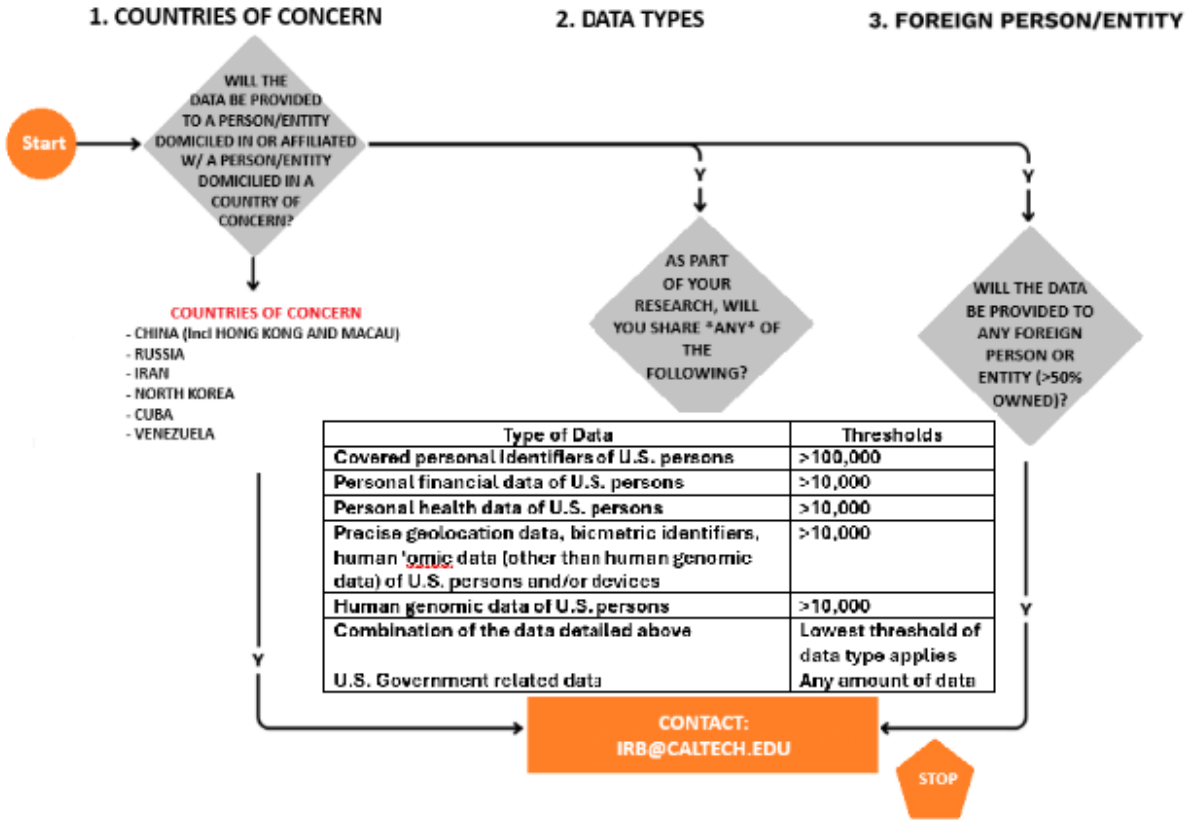
2. government-related data

If there is uncertainty, the data should be treated as covered and escalated for review.

*As part of your study, will you share any of the following:

Yes/No	Type of Data	Thresholds
Yes No	Covered personal identifiers of US persons	>90,000
Yes No	Personal financial data of US persons	>9,000
Yes No	Personal health data of US persons	>9,000
Yes No	Precise geolocation data, biometric identifiers, human 'omic data (other than human genomic data) of US persons and/or devices	>1,000
Yes No	Human genomic data of US persons	>100
Yes No	Combination of the data detailed above	Lowest threshold of data type applies
Yes No	U.S. Government-related data • Data linked to U.S. government personnel or contractors • Data related to sensitive government locations or operations	Any amount of data

Use the following flowchart to help you answer the questions above:



D. Prohibited Activities

If you would like to transfer covered data to a covered person or entity, you must contact the IRB office immediately at irb@caltech.edu to determine whether or not this transfer is possible.

E. Incident Reporting

Any suspected violation of the DOJ Bulk Data Rule must be reported immediately to the IRB office at irb@caltech.edu.