

States legal tradition, and not any other source of law.

(b) In a DPRC panel's review of an application under §201.9, the DPRC panel shall be guided by relevant decisions of the United States Supreme Court in the same way as are courts established under Article III of the United States Constitution, including those decisions regarding appropriate deference to relevant determinations of national security officials.

§ 201.11 Information security and classified national security information.

(a) All proceedings before and other activities of the DPRC and all activities of the Special Advocates shall be governed by Executive Order 13526 of December 29, 2009, "Classified National Security Information," or any successor order, and this part.

(b) Judges may serve on a DPRC panel convened under §201.7(a), and Special Advocates may be selected to assist a DPRC panel under §201.8(a), only if they hold the requisite security clearances to access classified national security information. The DPRC and Special Advocates shall have no authority to declassify or grant any person access to any classified or otherwise privileged or protected information, including the information reviewed in or information about the existence or outcome of any proceedings before the DPRC or any information that would tend to reveal whether a complainant was subject to signals intelligence activities.

(c) The Department of Justice Security Officer shall be responsible for establishing security procedures for proceedings before and other activities of the DPRC and the Special Advocate, and for amending those procedures as necessary.

§ 201.12 Disclaimer.

This part governs the ability to obtain review of the ODNI CLPO's determinations by the DPRC in accordance with the redress mechanism established in section 3 of the Executive order of October 7, 2022. This part is not intended to, and does not, create any other entitlement, right, or benefit, substantive or procedural, enforceable at law or in equity by any party

against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person. This part is not intended to, and does not, modify the availability or scope of any judicial review of the decisions rendered through the redress mechanism, which is governed by existing law.

PART 202—ACCESS TO U.S. SENSITIVE PERSONAL DATA AND GOVERNMENT-RELATED DATA BY COUNTRIES OF CONCERN OR COVERED PERSONS

Subpart A—General

Sec.

- 202.101 Scope.
- 202.102 Rules of construction and interpretation.
- 202.103 Relation of this part to other laws and regulations.
- 202.104 Delegation of authorities.
- 202.105 Amendment, modification, or revocation.
- 202.106 Severability.

Subpart B—Definitions

- 202.201 Access.
- 202.202 Attorney General.
- 202.203 Assistant Attorney General.
- 202.204 Biometric identifiers.
- 202.205 Bulk.
- 202.206 Bulk U.S. sensitive personal data.
- 202.207 CFIUS action.
- 202.208 China.
- 202.209 Country of concern.
- 202.210 Covered data transaction.
- 202.211 Covered person.
- 202.212 Covered personal identifiers.
- 202.213 Cuba.
- 202.214 Data brokerage.
- 202.215 Directing.
- 202.216 Effective date.
- 202.217 Employment agreement.
- 202.218 Entity.
- 202.219 Exempt transaction.
- 202.220 Former senior official.
- 202.221 Foreign person.
- 202.222 Government-related data.
- 202.223 Human biospecimens.
- 202.224 Human 'omic data.
- 202.225 IEEPA.
- 202.226 Information or informational materials.
- 202.227 Interest.
- 202.228 Investment agreement.
- 202.229 Iran.
- 202.230 Knowingly.
- 202.231 Licenses; general and specific.
- 202.232 Linked.

Pt. 202

- 202.233 Linkable.
- 202.234 Listed identifier.
- 202.235 National Security Division.
- 202.236 North Korea.
- 202.237 Order.
- 202.238 Person.
- 202.239 Personal communications.
- 202.240 Personal financial data.
- 202.241 Personal health data.
- 202.242 Precise geolocation data.
- 202.243 Prohibited transaction.
- 202.244 Property; property interest.
- 202.245 Recent former employees or contractors.
- 202.246 Restricted transaction.
- 202.247 Russia.
- 202.248 Security requirements.
- 202.249 Sensitive personal data.
- 202.250 Special Administrative Region of Hong Kong.
- 202.251 Special Administrative Region of Macau.
- 202.252 Telecommunications service.
- 202.253 Transaction.
- 202.254 Transfer.
- 202.255 United States.
- 202.256 United States person or U.S. person.
- 202.257 U.S. device.
- 202.258 Vendor agreement.
- 202.259 Venezuela.

Subpart C—Prohibited Transactions and Related Activities

- 202.301 Prohibited data-brokerage transactions.
- 202.302 Other prohibited data-brokerage transactions involving potential onward transfer to countries of concern or covered persons.
- 202.303 Prohibited human 'omic data and human biospecimen transactions.
- 202.304 Prohibited evasions, attempts, causing violations, and conspiracies.
- 202.305 Knowingly directing prohibited or restricted transactions.

Subpart D—Restricted Transactions

- 202.401 Authorization to conduct restricted transactions.
- 202.402 [Reserved]

Subpart E—Exempt Transactions

- 202.501 Personal communications.
- 202.502 Information or informational materials.
- 202.503 Travel.
- 202.504 Official business of the United States Government.
- 202.505 Financial services.
- 202.506 Corporate group transactions.
- 202.507 Transactions required or authorized by Federal law or international agreements, or necessary for compliance with Federal law.

28 CFR Ch. I (7-1-25 Edition)

- 202.508 Investment agreements subject to a CFIUS action.
- 202.509 Telecommunications services.
- 202.510 Drug, biological product, and medical device authorizations.
- 202.511 Other clinical investigations and post-marketing surveillance data.

Subpart F—Determination of Countries of Concern

- 202.601 Determination of countries of concern.

Subpart G—Covered Persons

- 202.701 Designation of covered persons.
- 202.702 Procedures governing removal from the Covered Persons List.

Subpart H—Licensing

- 202.801 General licenses.
- 202.802 Specific licenses.
- 202.803 General provisions.

Subpart I—Advisory Opinions

- 202.901 Inquiries concerning application of this part.

Subpart J—Due Diligence and Audit Requirements

- 202.1001 Due diligence for restricted transactions.
- 202.1002 Audits for restricted transactions.

Subpart K—Reporting and Recordkeeping Requirements

- 202.1101 Records and recordkeeping requirements.
- 202.1102 Reports to be furnished on demand.
- 202.1103 Annual reports.
- 202.1104 Reports on rejected prohibited transactions.

Subpart L—Submitting Applications, Requests, Reports, and Responses

- 202.1201 Procedures.

Subpart M—Penalties and Finding of Violation

- 202.1301 Penalties for violations.
- 202.1302 Process for pre-penalty notice.
- 202.1303 Penalty imposition.
- 202.1304 Administrative collection and litigation.
- 202.1305 Finding of violation.
- 202.1306 Opportunity to respond to a pre-penalty notice or finding of violation.

Department of Justice

Subpart N—Government-Related Location Data List

202.1401 Government-Related Location Data List.

AUTHORITY: 50 U.S.C. 1701 *et seq.*; 50 U.S.C. 1601 *et seq.*; E.O. 14117, 89 FR 15421.

SOURCE: 90 FR 1706, Jan. 8, 2025, unless otherwise noted.

Subpart A—General

§ 202.101 Scope.

(a) Executive Order 14117 of February 28, 2024 (Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern) ("the Order"), directs the Attorney General to issue regulations that prohibit or otherwise restrict United States persons from engaging in any acquisition, holding, use, transfer, transportation, or exportation of, or dealing in, any property in which a foreign country or national thereof has any interest ("transaction"), where the transaction involves United States Government-related data ("government-related data") or bulk U.S. sensitive personal data, as defined by final rules implementing the Order; falls within a class of transactions that has been determined by the Attorney General to pose an unacceptable risk to the national security of the United States because the transactions may enable access by countries of concern or covered persons to government-related data or bulk U.S. sensitive personal data; and meets other criteria specified by the Order.

(b) This part contains regulations implementing the Order and addressing the national emergency declared in Executive Order 13873 of May 15, 2019 (Securing the Information and Communications Technology and Services Supply Chain), and further addressed with additional measures in Executive Order 14034 of June 9, 2021 (Protecting Americans' Sensitive Data from Foreign Adversaries) and Executive Order 14117.

§ 202.102 Rules of construction and interpretation.

(a) The examples included in this part are provided for informational purposes and should not be construed

§ 202.106

to alter the meaning of the text of the regulations in this part.

(b) As used in this part, the term "including" means "including but not limited to."

(c) All references to "days" in this part mean calendar days. In computing any time period specified in this part:

(1) Exclude the day of the event that triggers the period;

(2) Count every day, including Saturdays, Sundays, and legal holidays; and

(3) Include the last day of the period, but if the last day is a Saturday, Sunday, or Federal holiday, the period continues to run until the end of the next day that is not a Saturday, Sunday, or Federal holiday.

§ 202.103 Relation of this part to other laws and regulations.

Nothing in this part shall be construed as altering or affecting any other authority, process, regulation, investigation, enforcement measure, or review provided by or established under any other provision of Federal law, including the International Emergency Economic Powers Act.

§ 202.104 Delegation of authorities.

Any action that the Attorney General is authorized to take pursuant to the Order or pursuant to this part may be taken by the Assistant Attorney General for National Security or by any other person to whom the Attorney General or Assistant Attorney General for National Security in writing delegates authority so to act.

§ 202.105 Amendment, modification, or revocation.

Except as otherwise provided by law, any determinations, prohibitions, decisions, licenses (whether general or specific), guidance, authorizations, instructions, orders, or forms issued pursuant to this part may be amended, modified, or revoked, in whole or in part, at any time.

§ 202.106 Severability.

If any provision of this part is held to be invalid or unenforceable by its terms, or as applied to any person or circumstance, or stayed pending further agency action or judicial review, the provision is to be construed so as

§ 202.201

to continue to give the maximum effect to the provision permitted by law, unless such holding will be one of utter invalidity or unenforceability, in which event the provision will be severable from this part and will not affect the remainder thereof.

Subpart B—Definitions

§ 202.201 Access.

The term *access* means 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. For purposes of determining whether a transaction is a covered data transaction, access is determined without regard for the application or effect of any security requirements.

§ 202.202 Attorney General.

The term *Attorney General* means the Attorney General of the United States or the Attorney General's designee.

§ 202.203 Assistant Attorney General.

The term *Assistant Attorney General* means the Assistant Attorney General, National Security Division, United States Department of Justice, or the Assistant Attorney General's designee.

§ 202.204 Biometric identifiers.

The term *biometric identifiers* means measurable physical characteristics or behaviors used to recognize or verify the identity of an individual, including facial images, voice prints and patterns, retina and iris scans, palm prints and fingerprints, gait, and keyboard usage patterns that are enrolled in a biometric system and the templates created by the system.

§ 202.205 Bulk.

The term *bulk* means any amount of sensitive personal data that meets or exceeds the following thresholds at any point in the preceding 12 months, whether through a single covered data transaction or aggregated across covered data transactions involving the

28 CFR Ch. I (7-1-25 Edition)

same U.S. person and the same foreign person or covered person:

(a) Human 'omic data collected about or maintained on more than 1,000 U.S. persons, or, in the case of human genomic data, more than 100 U.S. persons;

(b) Biometric identifiers collected about or maintained on more than 1,000 U.S. persons;

(c) Precise geolocation data collected about or maintained on more than 1,000 U.S. devices;

(d) Personal health data collected about or maintained on more than 10,000 U.S. persons;

(e) Personal financial data collected about or maintained on more than 10,000 U.S. persons;

(f) Covered personal identifiers collected about or maintained on more than 100,000 U.S. persons; or

(g) Combined data, meaning any collection or set of data that contains more than one of the categories in paragraphs (a) through (f) of this section, or that contains any listed identifier linked to categories in paragraphs (a) through (e) of this section, where any individual data type meets the threshold number of persons or devices collected or maintained in the aggregate for the lowest number of U.S. persons or U.S. devices in that category of data.

§ 202.206 Bulk U.S. sensitive personal data.

The term *bulk U.S. sensitive personal data* means a collection or set of sensitive personal data relating to U.S. persons, in any format, regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted, where such data meets or exceeds the applicable threshold set forth in § 202.205.

§ 202.207 CFIUS action.

The term *CFIUS action* means any agreement or condition the Committee on Foreign Investment in the United States has entered into or imposed pursuant to 50 U.S.C. 4565(l)(1), (3), or (5) to resolve a national security risk involving access by a country of concern or covered person to sensitive personal data that the Committee on Foreign Investment in the United States has

Department of Justice**§ 202.211**

explicitly designated, in the agreement or document containing the condition, as a CFIUS action, including:

- (a) Suspension of a proposed or pending transaction, as authorized under 50 U.S.C. 4565(l)(1);
- (b) Entry into or imposition of any agreement or condition with any party to a covered transaction, as authorized under 50 U.S.C. 4565(l)(3); and
- (c) The establishment of interim protections for covered transactions withdrawn before CFIUS's review or investigation is completed, as authorized under 50 U.S.C. 4565(l)(5).

§ 202.208 China.

The term *China* means the People's Republic of China, including the Special Administrative Region of Hong Kong and the Special Administrative Region of Macau, as well as any political subdivision, agency, or instrumentality thereof.

§ 202.209 Country of concern.

The term *country of concern* means any foreign government that, as determined by the Attorney General with the concurrence of the Secretary of State and the Secretary of Commerce:

- (a) Has engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons; and
- (b) Poses a significant risk of exploiting government-related data or bulk U.S. sensitive personal data to the detriment of the national security of the United States or security and safety of U.S. persons.

§ 202.210 Covered data transaction.

(a) *Definition.* A *covered data transaction* is any transaction that involves any access by a country of concern or covered person to any government-related data or bulk U.S. sensitive personal data and that involves:

- (1) Data brokerage;
- (2) A vendor agreement;
- (3) An employment agreement; or
- (4) An investment agreement.

(b) *Examples*—(1) *Example 1.* A U.S. institution conducts medical research at its own laboratory in a country of concern, including sending several U.S.-

citizen employees to that laboratory to perform and assist with the research. The U.S. institution does not engage in data brokerage or a vendor, employment, or investment agreement that gives a covered person or country of concern access to government-related data or bulk U.S. sensitive personal data. Because the U.S. institution does not engage in any data brokerage or enter into a vendor, employment, or investment agreement, the U.S. institution's research activity is not a covered data transaction.

(2) *Example 2.* A U.S. person engages in a vendor agreement with a covered person involving access to bulk U.S. sensitive personal data. The vendor agreement is a restricted transaction. To comply with the CISA security requirements, the U.S. person, among other things, uses data-level requirements to mitigate the risk that the covered person could access the data. The vendor agreement remains a covered data transaction subject to the requirements of this part.

(3) *Example 3.* A covered person engages in a vendor agreement with a U.S. person involving the U.S. person accessing bulk U.S. sensitive personal data already possessed by the covered person. The vendor agreement is not a covered data transaction because the transaction does not involve access by the covered person.

§ 202.211 Covered person.

(a) *Definition.* The term *covered person* means:

(1) A foreign person that is an entity that is 50% or more owned, directly or indirectly, individually or in the aggregate, by one or more countries of concern or persons described in paragraph (a)(2) of this section; or that is organized or chartered under the laws of, or has its principal place of business in, a country of concern;

(2) A foreign person that is an entity that is 50% or more owned, directly or indirectly, individually or in the aggregate, by one or more persons described in paragraphs (a)(1), (3), (4), or (5) of this section;

(3) A foreign person that is an individual who is an employee or contractor of a country of concern or of an

§ 202.211

entity described in paragraphs (a)(1), (2), or (5) of this section;

(4) A foreign person that is an individual who is primarily a resident in the territorial jurisdiction of a country of concern; or

(5) Any person, wherever located, determined by the Attorney General:

(i) To be, to have been, or to be likely to become owned or controlled by or subject to the jurisdiction or direction of a country of concern or covered person;

(ii) To act, to have acted or purported to act, or to be likely to act for or on behalf of a country of concern or covered person; or

(iii) To have knowingly caused or directed, or to be likely to knowingly cause or direct a violation of this part.

(b) *Examples*—(1) *Example 1*. Foreign persons primarily resident in Cuba, Iran, or another country of concern would be covered persons.

(2) *Example 2*. Chinese or Russian citizens located in the United States would be treated as U.S. persons and would not be covered persons (except to the extent individually designated). They would be subject to the same prohibitions and restrictions as all other U.S. persons with respect to engaging in covered data transactions with countries of concern or covered persons.

(3) *Example 3*. Citizens of a country of concern who are primarily resident in a third country, such as Russian citizens primarily resident in a European Union country or Cuban citizens primarily resident in a South American country that is not a country of concern, would not be covered persons except to the extent they are individually designated or to the extent that they are employees or contractors of a country of concern government or a covered person that is an entity.

(4) *Example 4*. A foreign person is located abroad and is employed by a company headquartered in China. Because the company is a covered person that is an entity and the employee is located outside the United States, the employee is a covered person.

(5) *Example 5*. A foreign person is located abroad and is employed by a company that has been designated as a covered person. Because the foreign person is the employee of a covered

28 CFR Ch. I (7-1-25 Edition)

person that is an entity and the employee is a foreign person, the person is a covered person.

(6) *Example 6*. A foreign person individual investor who principally resides in Venezuela owns 50% of a technology company that is solely organized under the laws of the United States. The investor is a covered person because the investor is a foreign person that is an individual who is primarily a resident in the territorial jurisdiction of a country of concern. The technology company is a U.S. person because it is an entity organized solely under the laws of the United States or any jurisdiction within the United States. The technology company is not a covered person because it is not a foreign person and therefore does not meet the criteria of § 202.211(a)(2). However, the technology company could still be designated as a covered person following a determination that the technology company meets one or more criteria of § 202.211(a)(5).

(7) *Example 7*. Same as Example 6, but the technology company is additionally organized under the laws of Luxembourg. A U.S. company wishes to license bulk U.S. sensitive personal data to the technology company. The technology company is not a U.S. person because it is not solely organized under the laws of the United States. The technology company is a covered person because it is 50% or more owned, directly or indirectly, individually or in the aggregate, by a foreign person that is an individual who is primarily resident in the territorial jurisdiction of a country of concern. The transaction between the U.S. company and the technology company would be a prohibited data transaction.

(8) *Example 8*. A foreign person that lives in China owns 50% of Foreign Entity A. Foreign Entity A owns 100% of Foreign Entity B and 100% of Foreign Entity C. Foreign Entity B owns 20% of Foreign Entity D. Foreign Entity C owns 30% of Foreign Entity D. Foreign Entity D would be a covered person for two independent reasons. First, Foreign Entity D because it is “indirectly” 50% or more owned by Foreign Entity A (20% through Foreign Entity B and 30% through Foreign Entity C). Second, Foreign Entity D is directly

50% owned, in the aggregate, by Foreign Entity B and Foreign Entity C, each of which are covered persons because they are 50% or more owned by Foreign Entity A.

§ 202.212 Covered personal identifiers.

(a) *Definition.* The term *covered personal identifiers* means any listed identifier:

(1) In combination with any other listed identifier; or

(2) In combination with other data that is disclosed by a transacting party pursuant to the transaction such that the listed identifier is linked or linkable to other listed identifiers or to other sensitive personal data.

(b) *Exclusion.* The term *covered personal identifiers* excludes:

(1) Demographic or contact data that is linked only to other demographic or contact data (such as first and last name, birthplace, ZIP code, residential street or postal address, phone number, and email address and similar public account identifiers); and

(2) A network-based identifier, account-authentication data, or call-detail data that is linked only to other network-based identifier, account-authentication data, or call-detail data as necessary for the provision of telecommunications, networking, or similar service.

(c) *Examples of listed identifiers in combination with other listed identifiers—*(1) *Example 1.* A standalone listed identifier in isolation (i.e., that is not linked to another listed identifier, sensitive personal data, or other data that is disclosed by a transacting party pursuant to the transaction such that the listed identifier is linked or linkable to other listed identifiers or to other sensitive personal data)—such as a Social Security Number or account username—would not constitute a covered personal identifier.

(2) *Example 2.* A listed identifier linked to another listed identifier—such as a first and last name linked to a Social Security number, a driver's license number linked to a passport number, a device Media Access Control ("MAC") address linked to a residential address, an account username linked to a first and last name, or a mobile advertising ID linked to an

email address—would constitute covered personal identifiers.

(3) *Example 3.* Demographic or contact data linked only to other demographic or contact data—such as a first and last name linked to a residential street address, an email address linked to a first and last name, or a customer loyalty membership record linking a first and last name to a phone number—would not constitute covered personal identifiers.

(4) *Example 4.* Demographic or contact data linked to other demographic or contact data and to another listed identifier—such as a first and last name linked to an email address and to an IP address—would constitute covered personal identifiers.

(5) *Example 5.* Account usernames linked to passwords as part of a sale of a dataset would constitute covered personal identifiers. Those pieces of account-authentication data are not linked as a necessary part of the provision of telecommunications, networking, or similar services. This combination would constitute covered personal identifiers.

(d) *Examples of a listed identifier in combination with other data disclosed by a transacting party—*(1) *Example 1.* A foreign person who is a covered person asks a U.S. company for a list of Media Access Control ("MAC") addresses from devices that have connected to the wireless network of a U.S. fast-food restaurant located in a particular government building. The U.S. company then sells the list of MAC addresses, without any other listed identifiers or sensitive personal data, to the covered person. The disclosed MAC addresses, when paired with the other data disclosed by the covered person—that the devices "have connected to the wireless network of a U.S. fast-food restaurant located in a particular government building"—makes it so that the MAC addresses are linked or linkable to other sensitive personal data, in this case precise geolocation data of the location of the fast-food restaurant that the national security-related individuals frequent with their devices. This combination of data therefore meets the definition of covered personal identifiers.

§ 202.213

(2) *Example 2.* A U.S. company sells to a country of concern a list of residential addresses that the company describes (whether in a heading on the list or separately to the country of concern as part of the transaction) as “addresses of members of a country of concern’s opposition political party in New York City” or as “addresses of active-duty military officers who live in Howard County, Maryland” without any other listed identifiers or sensitive personal data. The data disclosed by the U.S. company’s description, when paired with the disclosed addresses, makes the addresses linked or linkable to other listed identifiers or to other sensitive personal data of the U.S. individuals associated with them. This combination of data therefore meets the definition of covered personal identifiers.

(3) *Example 3.* A covered person asks a U.S. company for a bulk list of birth dates for “any American who visited a Starbucks in Washington, DC, in December 2023.” The U.S. company then sells the list of birth dates, without any other listed identifiers or sensitive personal data, to the covered person. The other data disclosed by the covered person—“any American who visited a Starbucks in Washington, DC, in December 2023”—does not make the birth dates linked or linkable to other listed identifiers or to other sensitive personal data. This combination of data therefore does not meet the definition of covered personal identifiers.

(4) *Example 4.* Same as Example 3, but the covered person asks the U.S. company for a bulk list of names (rather than birth dates) for “any American who visited a Starbucks in Washington, DC in December 2023.” The other data disclosed by the covered person—“any American who visited a Starbucks in Washington, DC, in December 2023”—does not make the list of names, without more, linked or linkable to other listed identifiers or to other sensitive personal data. This combination of data therefore does not meet the definition of covered personal identifiers.

(5) *Example 5.* A U.S. company sells to a covered person a list of residential addresses that the company describes (in a heading in the list or to the cov-

28 CFR Ch. I (7-1-25 Edition)

ered person as part of the transaction) as “households of Americans who watched more than 50% of episodes” of a specific popular TV show, without any other listed identifiers or sensitive personal data. The other data disclosed by the U.S. company—“Americans who watched more than 50% of episodes” of a specific popular TV show—does not increase the extent to which the addresses are linked or linkable to other listed identifiers or to other sensitive personal data. This combination of data therefore does not meet the definition of covered personal identifiers.

§ 202.213 Cuba.

The term *Cuba* means the Republic of Cuba, as well as any political subdivision, agency, or instrumentality thereof.

§ 202.214 Data brokerage.

(a) *Definition.* The term *data brokerage* means the sale of data, licensing of access to data, or similar commercial transactions, excluding an employment agreement, investment agreement, or a vendor agreement, involving the transfer of data from any person (the provider) to any other person (the recipient), where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data.

(b) *Examples*—(1) *Example 1.* A U.S. company sells bulk U.S. sensitive personal data to an entity headquartered in a country of concern. The U.S. company engages in prohibited data brokerage.

(2) *Example 2.* A U.S. company enters into an agreement that gives a covered person a license to access government-related data held by the U.S. company. The U.S. company engages in prohibited data brokerage.

(3) *Example 3.* A U.S. organization maintains a database of bulk U.S. sensitive personal data and offers annual memberships for a fee that provide members a license to access that data. Providing an annual membership to a covered person that includes a license to access government-related data or bulk U.S. sensitive personal data would constitute prohibited data brokerage.

(4) *Example 4.* A U.S. company owns and operates a mobile app for U.S.

users with available advertising space. As part of selling the advertising space, the U.S. company provides IP addresses and advertising IDs of more than 100,000 U.S. users' devices to an advertising exchange based in a country of concern in a twelve-month period. The U.S. company's provision of this data as part of the sale of advertising space is a covered data transaction involving data brokerage and is a prohibited transaction because IP addresses and advertising IDs are listed identifiers that satisfy the definition of bulk covered personal identifiers in this transaction.

(5) *Example 5.* Same as Example 4, but the U.S. company provides the data to an advertising exchange based in the United States. As part of the sale of the advertising space, the U.S. advertising exchange provides the data to advertisers headquartered in a country of concern. The U.S. company's provision of the data to the U.S. advertising exchange would not be a transaction because it is between U.S. persons. The advertising exchange's provision of this data to the country of concern-based advertisers is data brokerage because it is a commercial transaction involving the transfer of data from the U.S. advertising exchange to the advertisers headquartered in the country of concern, where those country-of-concern advertisers did not collect or process the data directly from the individuals linked or linkable to the collected or processed data. Furthermore, the U.S. advertising exchange's provision of this data to the country of concern-based advertisers is a prohibited transaction.

(6) *Example 6.* A U.S. information technology company operates an autonomous driving platform that collects the precise geolocation data of its cars operating in the United States. The U.S. company sells or otherwise licenses this bulk data to its parent company headquartered in a country of concern to help develop artificial intelligence technology and machine learning capabilities. The sale or license is data brokerage and a prohibited transaction.

(7) *Example 7.* A U.S. company owns or operates a mobile app or website for U.S. users. That mobile app or website contains one or more tracking pixels or

software development kits that were knowingly installed or approved for incorporation into the app or website by the U.S. company. The tracking pixels or software development kits transfer or otherwise provide access to government-related data or bulk U.S. sensitive personal data to a country of concern or covered person-owned social media app for targeted advertising. The U.S. company engages in prohibited data brokerage.

(8) *Example 8.* A non-U.S. company is contracted to develop a mobile app for a U.S. company. In developing the mobile app for that U.S. company, the non-U.S. company knowingly incorporates tracking pixels or software development kits into the mobile app that then transfer or otherwise provide access to government-related data or bulk U.S. sensitive personal data to a country of concern or covered person for targeted advertising, at the request of the U.S. company. The non-U.S. company has caused a violation of the data brokerage prohibition. If the U.S. company knowingly arranged the transfer of such data to the country of concern or covered person by requesting incorporation of the tracking pixels or software development kits, the U.S. company has engaged in prohibited data brokerage.

(9) *Example 9.* A U.S. researcher shares bulk human 'omic data on U.S. persons with a researcher in a country of concern (a covered person) with whom the U.S. researcher is drafting a paper for submission to an academic journal. The two researchers exchange country of concern and bulk U.S. human 'omic data over a period of several months to analyze and describe the findings of their research for the journal article. The U.S. person does not provide to or receive from the covered person or the covered person's employer any money or other valuable consideration as part of the authors' study. The U.S. person has not engaged in a covered data transaction involving data brokerage, because the transaction does not involve the sale of data, licensing of access to data, or similar commercial transaction involving the transfer of data to the covered person.

§ 202.215

(10) *Example 10.* A U.S. researcher receives a grant from a university in a country of concern to study bulk personal health data and bulk human genomic data on U.S. persons. The grant directs the researcher to share the underlying bulk U.S. sensitive personal data with the country of concern university (a covered person). The transaction is a covered data transaction because it involves access by a covered person to bulk U.S. sensitive personal data and is data brokerage because it involves the transfer of bulk U.S. sensitive personal data to a covered person in return for a financial benefit.

§ 202.215 Directing.

The term *directing* means having any authority (individually or as part of a group) to make decisions for or on behalf of an entity and exercising that authority.

§ 202.216 Effective date.

The term *effective date* refers to the effective date of this part, which is 12:01 a.m. ET on April 8, 2025.

§ 202.217 Employment agreement.

(a) *Definition.* The term *employment agreement* means any agreement or arrangement in which an individual, other than as an independent contractor, performs work or performs job functions directly for a person in exchange for payment or other consideration, including employment on a board or committee, executive-level arrangements or services, and employment services at an operational level.

(b) *Examples—(1) Example 1.* A U.S. company that conducts consumer human genomic testing collects and maintains bulk human genomic data from U.S. consumers. The U.S. company has global IT operations, including employing a team of individuals who are citizens of and primarily resident in a country of concern to provide back-end services. The agreements related to employing these individuals are employment agreements. Employment as part of the global IT operations team includes access to the U.S. company's systems containing the bulk human genomic data. These employment agreements would be prohibited

28 CFR Ch. I (7-1-25 Edition)

transactions (because they involve access to bulk human genomic data).

(2) *Example 2.* A U.S. company develops its own mobile games and social media apps that collect the bulk U.S. sensitive personal data of its U.S. users. The U.S. company distributes these games and apps in the United States through U.S.-based digital distribution platforms for software applications. The U.S. company intends to hire as CEO an individual designated by the Attorney General as a covered person because of evidence the CEO acts on behalf of a country of concern. The agreement retaining the individual as CEO would be an employment agreement. The individual's authorities and responsibilities as CEO involve access to all data collected by the apps, including the bulk U.S. sensitive personal data. The CEO's employment would be a restricted transaction.

(3) *Example 3.* A U.S. company has derived U.S. persons' biometric identifiers by scraping public photos from social media platforms. The U.S. company stores the derived biometric identifiers in bulk, including face-data scans, for the purpose of training or enhancing facial-recognition software. The U.S. company intends to hire a foreign person, who primarily resides in a country of concern, as a project manager responsible for the database. The agreement retaining the project manager would be an employment agreement. The individual's employment as the lead project manager would involve access to the bulk biometric identifiers. The project manager's employment would be a restricted transaction.

(4) *Example 4.* A U.S. financial-services company seeks to hire a data scientist who is a citizen of a country of concern who primarily resides in that country of concern and who is developing a new artificial intelligence-based personal assistant that could be sold as a standalone product to the company's customers. The arrangement retaining the data scientist would be an employment agreement. As part of that individual's employment, the data scientist would have administrator rights that allow that individual to access, download, and transmit bulk quantities of personal financial data not ordinarily incident to and

part of the company's underlying provision of financial services to its customers. The data scientist's employment would be a restricted transaction.

(5) *Example 5.* 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.

§ 202.218 Entity.

The term *entity* means a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization.

§ 202.219 Exempt transaction.

The term *exempt transaction* means a data transaction that is subject to one or more exemptions described in subpart E of this part.

§ 202.220 Former senior official.

The term *former senior official* means either a "former senior employee" or a "former very senior employee," as those terms are defined in 5 CFR 2641.104.

§ 202.221 Foreign person.

The term *foreign person* means any person that is not a U.S. person.

§ 202.222 Government-related data.

(a) *Definition.* The term *government-related data* means the following:

(1) Any precise geolocation data, regardless of volume, for any location within any area enumerated on the Government-Related Location Data List in § 202.1401 which the Attorney General has determined poses a heightened risk of being exploited by a country of concern to reveal insights about locations controlled by the Federal Government, including insights about facilities, activities, or populations in those locations, to the detriment of national security, because of the nature

of those locations or the personnel who work there. Such locations may include:

(i) The worksite or duty station of Federal Government employees or contractors who occupy a national security position as that term is defined in 5 CFR 1400.102(a)(4);

(ii) A military installation as that term is defined in 10 U.S.C. 2801(c)(4); or

(iii) Facilities or locations that otherwise support the Federal Government's national security, defense, intelligence, law enforcement, or foreign policy missions.

(2) Any sensitive personal data, regardless of volume, that a transacting party markets as linked or linkable to current or recent former employees or contractors, or former senior officials, of the United States Government, including the military and Intelligence Community.

(b) *Examples of government-related data marketed by a transacting party*—(1) *Example 1.* A U.S. company advertises the sale of a set of sensitive personal data as belonging to "active duty" personnel, "military personnel who like to read," "DoD" personnel, "government employees," or "communities that are heavily connected to a nearby military base." The data is government-related data.

(2) *Example 2.* In discussing the sale of a set of sensitive personal data with a covered person, a U.S. company describes the dataset as belonging to members of a specific named organization. The identified organization restricts membership to current and former members of the military and their families. The data is government-related data.

§ 202.223 Human biospecimens.

(a) The term *human biospecimens* means a quantity of tissue, blood, urine, or other human-derived material, including such material classified under any of the following 10-digit Harmonized System-based Schedule B numbers:

(1) 0501.00.0000 Human hair, unworked, whether or not washed or scoured; waste of human hair

(2) 3001.20.0000 Extracts of glands or other organs or of their secretions

§ 202.224

- (3) 3001.90.0115 Glands and other organs, dried, whether or not powdered
- (4) 3002.12.0010 Human blood plasma
- (5) 3002.12.0020 Normal human blood sera, whether or not freeze-dried
- (6) 3002.12.0030 Human immune blood sera
- (7) 3002.12.0090 Antisera and other blood fractions, Other
- (8) 3002.51.0000 Cell therapy products
- (9) 3002.59.0000 Cell cultures, whether or not modified, Other
- (10) 3002.90.5210 Whole human blood
- (11) 3002.90.5250 Blood, human/animal, other
- (12) 9705.21.0000 Human specimens and parts thereof

(b) Notwithstanding paragraph (a) of this section, the term *human biospecimens* does not include human biospecimens, including human blood, cell, and plasma-derived therapeutics, intended by a recipient solely for use in diagnosing, treating, or preventing any disease or medical condition.

§ 202.224 Human 'omic data.

(a) The term *human 'omic data* means:

(1) *Human genomic data*. Data representing the nucleic acid sequences that constitute the entire set or a subset of the genetic instructions found in a human cell, including the result or results of an individual's "genetic test" (as defined in 42 U.S.C. 300gg-91(d)(17)) and any related human genetic sequencing data.

(2) *Human epigenomic data*. Data derived from a systems-level analysis of human epigenetic modifications, which are changes in gene expression that do not involve alterations to the DNA sequence itself. These epigenetic modifications include modifications such as DNA methylation, histone modifications, and non-coding RNA regulation. Routine clinical measurements of epigenetic modifications for individualized patient care purposes would not be considered epigenomic data under this rule because such measurements would not entail a systems-level analysis of the epigenetic modifications in a sample.

(3) *Human proteomic data*. Data derived from a systems-level analysis of proteins expressed by a human genome, cell, tissue, or organism. Routine clinical measurements of proteins for individualized patient care purposes would not be considered proteomic data under this rule because such measurements would not entail a systems-level analysis of the proteins found in such a sample.

28 CFR Ch. I (7-1-25 Edition)

vidualized patient care purposes would not be considered proteomic data under this rule because such measurements would not entail a systems-level analysis of the proteins found in such a sample.

(4) *Human transcriptomic data*. Data derived from a systems-level analysis of RNA transcripts produced by the human genome under specific conditions or in a specific cell type. Routine clinical measurements of RNA transcripts for individualized patient care purposes would not be considered transcriptomic data under this rule because such measurements would not entail a systems-level analysis of the RNA transcripts in a sample.

(b) The term *human 'omic data* excludes pathogen-specific data embedded in human 'omic data sets.

§ 202.225 IEEPA.

The term *IEEPA* means the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*).

§ 202.226 Information or informational materials.

(a) *Definition*. The term *information or informational materials* is limited to expressive material and includes publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds. It does not include data that is technical, functional, or otherwise non-expressive.

(b) *Exclusions*. The term *information or informational materials* does not include:

(1) Information or informational materials not fully created and in existence at the date of the data transaction, or the substantive or artistic alteration or enhancement of information or informational materials, or the provision of marketing and business consulting services, including to market, produce or co-produce, or assist in the creation of information or informational materials;

(2) Items that were, as of April 30, 1994, or that thereafter become, controlled for export to the extent that such controls promote the non-proliferation or antiterrorism policies of the United States, or with respect to

which acts are prohibited by 18 U.S.C. chapter 37.

(c) *Examples*—(1) *Example 1*. A U.S. person enters into an agreement to create a customized dataset of bulk U.S. sensitive personal data that meets a covered person's specifications (such as the specific types and fields of data, date ranges, and other criteria) and to sell that dataset to the covered person. This customized dataset is not fully created and in existence at the date of the agreement, and therefore is not information or informational materials.

(2) *Example 2*. A U.S. company has access to several pre-existing databases of different bulk U.S. sensitive personal data. The U.S. company offers, for a fee, to use data analytics to link the data across these databases to the same individuals and to sell that combined dataset to a covered person. This service constitutes a substantive alteration or enhancement of the data in the pre-existing databases and therefore is not information or informational materials.

§ 202.227 Interest.

Except as otherwise provided in this part, the term *interest*, when used with respect to property (e.g., “an interest in property”), means an interest of any nature whatsoever, direct or indirect.

§ 202.228 Investment agreement.

(a) *Definition*. The term *investment agreement* means an agreement or arrangement in which any person, in exchange for payment or other consideration, obtains direct or indirect ownership interests in or rights in relation to:

(1) Real estate located in the United States; or

(2) A U.S. legal entity.

(b) *Exclusion for passive investments*. The term *investment agreement* excludes any investment that:

(1) Is made:

(i) Into a publicly traded security, with “security” defined in section 3(a)(10) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(10)), denominated in any currency that trades on a securities exchange or through the method of trading that is commonly referred to as “over-the-counter,” in any jurisdiction;

(ii) Into a security offered by:

(A) Any “investment company” (as defined in section 3(a)(1) of the Investment Company Act of 1940 (15 U.S.C. 80a-3(a)(1)) that is registered with the United States Securities and Exchange Commission, such as index funds, mutual funds, or exchange traded funds; or

(B) Any company that has elected to be regulated or is regulated as a business development company pursuant to section 54(a) of the Investment Company Act of 1940 (15 U.S.C. 80a-53), or any derivative of either of the foregoing; or

(iii) As a limited partner into a venture capital fund, private equity fund, fund of funds, or other pooled investment fund, or private entity, if the limited partner's contribution is solely capital and the limited partner cannot make managerial decisions, is not responsible for any debts beyond its investment, and does not have the formal or informal ability to influence or participate in the fund's or a U.S. person's decision making or operations;

(2) Gives the covered person less than 10% in total voting and equity interest in a U.S. person; and

(3) Does not give a covered person rights beyond those reasonably considered to be standard minority shareholder protections, including (a) membership or observer rights on, or the right to nominate an individual to a position on, the board of directors or an equivalent governing body of the U.S. person, or (b) any other involvement, beyond the voting of shares, in substantive business decisions, management, or strategy of the U.S. person.

(c) *Examples*—(1) *Example 1*. 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.

§ 202.229**28 CFR Ch. I (7-1-25 Edition)**

(2) *Example 2.* A foreign technology company that is subject to the jurisdiction of a country of concern and that the Attorney General has designated as a covered person enters into a shareholders' agreement with a U.S. business that develops mobile games and social media apps, acquiring a minority equity stake in the U.S. business. The shareholders' agreement is an investment agreement. These games and apps developed by the U.S. business systematically collect bulk U.S. sensitive personal data of its U.S. users. The investment agreement explicitly gives the foreign technology company the ability to access this data and is therefore a restricted transaction.

(3) *Example 3.* Same as Example 2, but the investment agreement either does not explicitly give the foreign technology company the right to access the data or explicitly forbids that access. The investment agreement nonetheless provides the foreign technology company with the sufficient ownership interest, rights, or other involvement in substantive business decisions, management, or strategy such that the investment does not constitute a passive investment. Because it is not a passive investment, the ownership interest, rights, or other involvement in substantive business decisions, management, or strategy gives the foreign technology company the ability to obtain logical or physical access, regardless of how the agreement formally distributes those rights. The investment agreement therefore involves access to bulk U.S. sensitive personal data. The investment agreement is a restricted transaction.

(4) *Example 4.* Same as Example 3, but the U.S. business does not maintain or have access to any government-related data or bulk U.S. sensitive personal data (e.g., a pre-commercial company or startup company). Because the data transaction cannot involve access to any government-related data or bulk U.S. sensitive personal data, this investment agreement does not meet the definition of a covered data transaction and is not a restricted transaction.

§ 202.229 Iran.

The term *Iran* means the Islamic Republic of Iran, as well as any political

subdivision, agency, or instrumentality thereof.

§ 202.230 Knowingly.

(a) *Definition.* The term *knowingly*, with respect to conduct, a circumstance, or a result, means that a person has actual knowledge, or reasonably should have known, of the conduct, the circumstance, or the result.

(b) *Examples*—(1) *Example 1.* A U.S. company sells DNA testing kits to U.S. consumers and maintains bulk human genomic data collected from those consumers. The U.S. company enters into a contract with a foreign cloud-computing company (which is not a covered person) to store the U.S. company's database of human genomic data. The foreign company hires employees from other countries, including citizens of countries of concern who primarily reside in a country of concern, to manage databases for its customers, including the U.S. company's human genomic database. There is no indication of evasion, such as the U.S. company knowingly directing the foreign company's employment agreements with covered persons, or the U.S. company engaging in and structuring these transactions to evade the regulations. The cloud-computing services agreement between the U.S. company and the foreign company would not be prohibited or restricted, because that covered data transaction is between a U.S. person and a foreign company that does not meet the definition of a covered person. The employment agreements between the foreign company and the covered persons would not be prohibited or restricted because those agreements are between foreign persons.

(2) *Example 2.* A U.S. company transmits the bulk U.S. sensitive personal data of U.S. persons to a country of concern, in violation of this part, using a fiber optic cable operated by another U.S. company. The U.S. cable operator has not knowingly engaged in a prohibited transaction or a restricted transaction solely by virtue of operating the fiber optic cable because the U.S. cable operator does not know, and reasonably should not know, the content of the traffic transmitted across the fiber optic cable.

(3) *Example 3.* A U.S. service provider provides a software platform on which a U.S. company processes the bulk U.S. sensitive personal data of its U.S.-person customers. While the U.S. service provider is generally aware of the nature of the U.S. company's business, the U.S. service provider is not aware of the kind or volume of data that the U.S. company processes on the platform, how the U.S. company uses the data, or whether the U.S. company engages in data transactions. The U.S. company also primarily controls access to its data on the platform, with the U.S. service provider accessing the data only for troubleshooting or technical support purposes, upon request by the U.S. company. Subsequently, without the actual knowledge of the U.S. service provider and without providing the U.S. service provider with any information from which the service provider should have known, the U.S. company grants access to the data on the U.S. service provider's software platform to a covered person through a covered data transaction, in violation of this part. The U.S. service provider itself, however, has not knowingly engaged in a restricted transaction by enabling the covered persons' access via its software platform.

(4) *Example 4.* Same as Example 3, but in addition to providing the software platform, the U.S. company's contract with the U.S. service provider also outsources the U.S. company's processing and handling of the data to the U.S. service provider. As a result, the U.S. service provider primarily controls access to the U.S. company's bulk U.S. sensitive personal data on the platform. The U.S. service provider employs a covered person and grants access to this data as part of this employment. Although the U.S. company's contract with the U.S. service provider is not a restricted transaction, the U.S. service provider's employment agreement with the covered person is a restricted transaction. The U.S. service provider has thus knowingly engaged in a restricted transaction by entering into an employment agreement that grants access to its employee because the U.S. service provider knew or should have known of its employee's covered person status and, as the party

responsible for processing and handling the data, the U.S. service provider was aware of the kind and volume of data that the U.S. company processes on the platform.

(5) *Example 5.* A U.S. company provides cloud storage to a U.S. customer for the encrypted storage of the customer's bulk U.S. sensitive personal data. The U.S. cloud-service provider has an emergency back-up encryption key for all its customers' data, but the company is contractually limited to using the key to decrypt the data only at the customer's request. The U.S. customer's systems and access to the key become disabled, and the U.S. customer requests that the cloud-service provider use the back-up encryption key to decrypt the data and store it on a backup server while the customer restores its own systems. By having access to and using the backup encryption key to decrypt the data in accordance with the contractual limitation, the U.S. cloud-service provider does not and reasonably should not know the kind and volumes of the U.S. customer's data. If the U.S. customer later uses the cloud storage to knowingly engage in a prohibited transaction, the U.S. cloud-service provider's access to and use of the backup encryption key does not mean that the U.S. cloud-service provider has also knowingly engaged in a restricted transaction.

(6) *Example 6.* A prominent human genomics research clinic enters into a cloud-services contract with a U.S. cloud-service provider that specializes in storing and processing healthcare data to store bulk human genomic research data. The cloud-service provider hires IT personnel in a country of concern, who are thus covered persons. While the data that is stored is encrypted, the IT personnel can access the data in encrypted form. The employment agreement between the U.S. cloud-service provider and the IT professionals in the country of concern is a prohibited transaction because the agreement involves giving the IT personnel access to the encrypted data and constitutes a transfer of human genomic data. Given the nature of the research institution's work and the cloud-service provider's expertise in

§ 202.231**28 CFR Ch. I (7-1-25 Edition)**

storing healthcare data, the cloud-service provider reasonably should have known that the encrypted data is bulk U.S. sensitive personal data covered by the regulations. The cloud-service provider has therefore knowingly engaged in a prohibited transaction (because it involves access to human genomic data).

§ 202.231 Licenses; general and specific.

(a) *General license.* The term *general license* means a written license issued pursuant to this part authorizing a class of transactions and not limited to a particular person.

(b) *Specific license.* The term *specific license* means a written license issued pursuant to this part to a particular person or persons, authorizing a particular transaction or transactions in response to a written license application.

§ 202.232 Linked.

(a) *Definition.* The term *linked* means associated.

(b) *Examples—(1) Example 1.* A U.S. person transfers two listed identifiers in a single spreadsheet—such as a list of names of individuals and associated MAC addresses for those individuals' devices. The names and MAC addresses would be considered linked.

(2) *Example 2.* A U.S. person transfers two listed identifiers in different spreadsheets—such as a list of names of individuals in one spreadsheet and MAC addresses in another spreadsheet—to two related parties in two different covered data transactions. The names and MAC addresses would be considered linked, provided that some correlation existed between the names and MAC addresses (e.g., associated employee ID number is also listed in both spreadsheets).

(3) *Example 3.* A U.S. person transfers a standalone list of MAC addresses, without any additional listed identifiers. The standalone list does not include covered personal identifiers. That standalone list of MAC addresses would not become covered personal identifiers even if the receiving party is capable of obtaining separate sets of other listed identifiers or sensitive personal data through separate covered

data transactions with unaffiliated parties that would ultimately permit the association of the MAC addresses to specific persons. The MAC addresses would not be considered linked or linkable to those separate sets of other listed identifiers or sensitive personal data.

§ 202.233 Linkable.

The term *linkable* means reasonably capable of being linked.

NOTE TO § 202.233: Data is considered linkable when the identifiers involved in a single covered data transaction, or in multiple covered data transactions or a course of dealing between the same or related parties, are reasonably capable of being associated with the same person(s). Identifiers are not linked or linkable when additional identifiers or data not involved in the relevant covered data transaction(s) would be necessary to associate the identifiers with the same specific person(s).

§ 202.234 Listed identifier.

The term *listed identifier* means any piece of data in any of the following data fields:

(a) Full or truncated government identification or account number (such as a Social Security number, driver's license or State identification number, passport number, or Alien Registration Number);

(b) Full financial account numbers or personal identification numbers associated with a financial institution or financial-services company;

(c) Device-based or hardware-based identifier (such as International Mobile Equipment Identity ("IMEI"), Media Access Control ("MAC") address, or Subscriber Identity Module ("SIM") card number);

(d) Demographic or contact data (such as first and last name, birth date, birthplace, ZIP code, residential street or postal address, phone number, email address, or similar public account identifiers);

(e) Advertising identifier (such as Google Advertising ID, Apple ID for Advertisers, or other mobile advertising ID ("MAID"));

(f) Account-authentication data (such as account username, account password, or an answer to security questions);

Department of Justice**§ 202.244**

(g) Network-based identifier (such as Internet Protocol (“IP”) address or cookie data); or

(h) Call-detail data (such as Customer Proprietary Network Information (“CPNI”)).

§ 202.235 National Security Division.

The term *National Security Division* means the National Security Division of the United States Department of Justice.

§ 202.236 North Korea.

The term *North Korea* means the Democratic People’s Republic of North Korea, and any political subdivision, agency, or instrumentality thereof.

§ 202.237 Order.

The term *Order* means Executive Order 14117 of February 28, 2024 (Preventing Access to Americans’ Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern), 89 FR 15421 (March 1, 2024).

§ 202.238 Person.

The term *person* means an individual or entity.

§ 202.239 Personal communications.

The term *personal communications* means any postal, telegraphic, telephonic, or other personal communication that does not involve the transfer of anything of value, as set out under 50 U.S.C. 1702(b)(1).

§ 202.240 Personal financial data.

The term *personal financial data* means data about an individual’s credit, charge, or debit card, or bank account, including purchases and payment history; data in a bank, credit, or other financial statement, including assets, liabilities, debts, or trades in a securities portfolio; or data in a credit report or in a “consumer report” (as defined in 15 U.S.C. 1681a(d)).

§ 202.241 Personal health data.

The term *personal health data* means health information that indicates, reveals, or describes the past, present, or future physical or mental health or condition of an individual; the provi-

sion of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual. This term includes basic physical measurements and health attributes (such as bodily functions, height and weight, vital signs, symptoms, and allergies); social, psychological, behavioral, and medical diagnostic, intervention, and treatment history; test results; logs of exercise habits; immunization data; data on reproductive and sexual health; and data on the use or purchase of prescribed medications.

§ 202.242 Precise geolocation data.

The term *precise geolocation data* means data, whether real-time or historical, that identifies the physical location of an individual or a device with a precision of within 1,000 meters.

§ 202.243 Prohibited transaction.

The term *prohibited transaction* means a data transaction that is subject to one or more of the prohibitions described in subpart C of this part.

§ 202.244 Property; property interest.

The terms *property* and *property interest* include money; checks; drafts; bullion; bank deposits; savings accounts; debts; indebtedness; obligations; notes; guarantees; debentures; stocks; bonds; coupons; any other financial instruments; bankers acceptances; mortgages, pledges, liens, or other rights in the nature of security; warehouse receipts, bills of lading, trust receipts, bills of sale, or any other evidences of title, ownership, or indebtedness; letters of credit and any documents relating to any rights or obligations thereunder; powers of attorney; goods; wares; merchandise; chattels; stocks on hand; ships; goods on ships; real estate mortgages; deeds of trust; vendors’ sales agreements; land contracts, leaseholds, ground rents, real estate and any other interest therein; options; negotiable instruments; trade acceptances; royalties; book accounts; accounts payable; judgments; patents; trademarks or copyrights; insurance policies; safe deposit boxes and their contents; annuities; pooling agreements; services of any nature whatsoever; contracts of

§ 202.245**28 CFR Ch. I (7-1-25 Edition)**

any nature whatsoever; any other property, real, personal, or mixed, tangible or intangible, or interest or interests therein, present, future, or contingent.

§ 202.245 Recent former employees or contractors.

The terms *recent former employees* or *recent former contractors* mean employees or contractors who worked for or provided services to the United States Government, in a paid or unpaid status, within the past 2 years of a potential covered data transaction.

§ 202.246 Restricted transaction.

The term *restricted transaction* means a data transaction that is subject to subpart D of this part.

§ 202.247 Russia.

The term *Russia* means the Russian Federation, and any political subdivision, agency, or instrumentality thereof.

§ 202.248 Security requirements.

The term *security requirements* means the Cybersecurity and Infrastructure Agency (“CISA”) Security Requirements for Restricted Transactions E.O. 14117 Implementation, January 2025. This material is incorporated by reference into this section with the approval of the Director of the Federal Register under 5 U.S.C. 552(a) and 1 CFR part 51. This incorporation by reference (“IBR”) material is available for inspection at the Department of Justice and at the National Archives and Records Administration (“NARA”). Please contact the Foreign Investment Review Section, National Security Division, U.S. Department of Justice, 175 N St. NE, Washington, DC 20002, telephone: 202-514-8648, NSD.FIRS.datasecurity@usdoj.gov; www.justice.gov/nsd. For information on the availability of this material at NARA, visit www.archives.gov/federal-register/cfr/ibr-locations or email fr.inspection@nara.gov. The material may be obtained from the National Security Division and the Cybersecurity and Infrastructure Security Agency (CISA), Mail Stop 0380, Department of Homeland Security, 245 Murray Lane, Washington, DC 20528-0380;

central@cisa.gov; 888-282-0870; www.cisa.gov/.

§ 202.249 Sensitive personal data.

(a) *Definition.* The term *sensitive personal data* means covered personal identifiers, precise geolocation data, biometric identifiers, human ‘omic data, personal health data, personal financial data, or any combination thereof.

(b) *Exclusions.* The term *sensitive personal data*, and each of the categories of *sensitive personal data*, excludes:

(1) Public or nonpublic data that does not relate to an individual, including such data that meets the definition of a “trade secret” (as defined in 18 U.S.C. 1839(3)) or “proprietary information” (as defined in 50 U.S.C. 1708(d)(7));

(2) Data that is, at the time of the transaction, lawfully available to the public from a Federal, State, or local government record (such as court records) or in widely distributed media (such as sources that are generally available to the public through unrestricted and open-access repositories);

(3) Personal communications; and

(4) Information or informational materials and ordinarily associated metadata or metadata reasonably necessary to enable the transmission or dissemination of such information or informational materials.

§ 202.250 Special Administrative Region of Hong Kong.

The term *Special Administrative Region of Hong Kong* means the Special Administrative Region of Hong Kong, and any political subdivision, agency, or instrumentality thereof.

§ 202.251 Special Administrative Region of Macau.

The term *Special Administrative Region of Macau* means the Special Administrative Region of Macau, and any political subdivision, agency, or instrumentality thereof.

§ 202.252 Telecommunications service.

The term *telecommunications service* means the provision of voice and data communications services regardless of format or mode of delivery, including communications services delivered over cable, Internet Protocol, wireless,

fiber, or other transmission mechanisms, as well as arrangements for network interconnection, transport, messaging, routing, or international voice, text, and data roaming.

§ 202.253 Transaction.

The term *transaction* means any acquisition, holding, use, transfer, transportation, exportation of, or dealing in any property in which a foreign country or national thereof has an interest.

§ 202.254 Transfer.

The term *transfer* means any actual or purported act or transaction, whether or not evidenced by writing, and whether or not done or performed within the United States, the purpose, intent, or effect of which is to create, surrender, release, convey, transfer, or alter, directly or indirectly, any right, remedy, power, privilege, or interest with respect to any property. Without limitation on the foregoing, it shall include the making, execution, or delivery of any assignment, power, conveyance, check, declaration, deed, deed of trust, power of attorney, power of appointment, bill of sale, mortgage, receipt, agreement, contract, certificate, gift, sale, affidavit, or statement; the making of any payment; the setting off of any obligation or credit; the appointment of any agent, trustee, or fiduciary; the creation or transfer of any lien; the issuance, docketing, filing, or levy of or under any judgment, decree, attachment, injunction, execution, or other judicial or administrative process or order, or the service of any garnishment; the acquisition of any interest of any nature whatsoever by reason of a judgment or decree of any foreign country; the fulfillment of any condition; the exercise of any power of appointment, power of attorney, or other power; or the acquisition, disposition, transportation, importation, exportation, or withdrawal of any security.

§ 202.255 United States.

The term *United States* means the United States, its territories and possessions, and all areas under the jurisdiction or authority thereof.

§ 202.256 United States person or U.S. person.

(a) *Definition.* The terms *United States person* and *U.S. person* mean any United States citizen, national, or lawful permanent resident; any individual admitted to the United States as a refugee under 8 U.S.C. 1157 or granted asylum under 8 U.S.C. 1158; any entity organized solely under the laws of the United States or any jurisdiction within the United States (including foreign branches); or any person in the United States.

(b) *Examples*—(1) *Example 1.* An individual is a citizen of a country of concern and is in the United States. The individual is a U.S. person.

(2) *Example 2.* An individual is a U.S. citizen. The individual is a U.S. person, regardless of location.

(3) *Example 3.* An individual is a dual citizen of the United States and a country of concern. The individual is a U.S. person, regardless of location.

(4) *Example 4.* An individual is a citizen of a country of concern, is not a permanent resident alien of the United States, and is outside the United States. The individual is a foreign person.

(5) *Example 5.* A company is organized under the laws of the United States and has a foreign branch in a country of concern. The company, including its foreign branch, is a U.S. person.

(6) *Example 6.* A parent company is organized under the laws of the United States and has a subsidiary organized under the laws of a country of concern. The subsidiary is a foreign person regardless of the degree of ownership by the parent company; the parent company is a U.S. person.

(7) *Example 7.* A company is organized under the laws of a country of concern and has a branch in the United States. The company, including its U.S. branch, is a foreign person.

(8) *Example 8.* A parent company is organized under the laws of a country of concern and has a subsidiary organized under the laws of the United States. The subsidiary is a U.S. person regardless of the degree of ownership by the parent company; the parent company is a foreign person.

§ 202.257

§ 202.257 U.S. device.

The term *U.S. device* means any device with the capacity to store or transmit data that is linked or linkable to a U.S. person.

§ 202.258 Vendor agreement.

(a) *Definition.* The term *vendor agreement* means any agreement or arrangement, other than an employment agreement, in which any person provides goods or services to another person, including cloud-computing services, in exchange for payment or other consideration.

(b) *Examples.*—(1) *Example 1.* A U.S. company collects bulk precise geolocation data from U.S. users through an app. The U.S. company enters into an agreement with a company headquartered in a country of concern to process and store this data. This vendor agreement is a restricted transaction.

(2) *Example 2.* A medical facility in the United States contracts with a company headquartered in a country of concern to provide IT-related services. The contract governing the provision of services is a vendor agreement. The medical facility has bulk personal health data on its U.S. patients. The IT services provided under the contract involve access to the medical facility's systems containing the bulk personal health data. This vendor agreement is a restricted transaction.

(3) *Example 3.* A U.S. company, which is owned by an entity headquartered in a country of concern and has been designated a covered person, establishes a new data center in the United States to offer managed services. The U.S. company's data center serves as a vendor to various U.S. companies to store bulk U.S. sensitive personal data collected by those companies. These vendor agreements are restricted transactions.

(4) *Example 4.* A U.S. company develops mobile games that collect bulk precise geolocation data and biometric identifiers of U.S.-person users. The U.S. company contracts part of the software development to a foreign person who is primarily resident in a country of concern and is a covered person. The contract with the foreign person is a vendor agreement. The software-development services provided by

28 CFR Ch. I (7-1-25 Edition)

the covered person under the contract involve access to the bulk precise geolocation data and biometric identifiers. This is a restricted transaction.

(5) *Example 5.* A U.S. multinational company maintains bulk U.S. sensitive personal data of U.S. persons. This company has a foreign branch, located in a country of concern, that has access to this data. The foreign branch contracts with a local company located in the country of concern to provide cleaning services for the foreign branch's facilities. The contract is a vendor agreement, the foreign branch is a U.S. person, and the local company is a covered person. Because the services performed under this vendor agreement do not "involve access to" the bulk U.S. sensitive personal data, the vendor agreement would not be a covered data transaction.

§ 202.259 Venezuela.

The term *Venezuela* means the Bolivarian Republic of Venezuela, and any political subdivision, agency, or instrumentality thereof.

Subpart C—Prohibited Transactions and Related Activities

§ 202.301 Prohibited data-brokerage transactions.

(a) *Prohibition.* Except as otherwise authorized pursuant to subparts E or H of this part or any other provision of this part, no U.S. person, on or after the effective date, may knowingly engage in a covered data transaction involving data brokerage with a country of concern or covered person.

(b) *Examples.*—(1) *Example 1.* A U.S. subsidiary of a company headquartered in a country of concern develops an artificial intelligence chatbot in the United States that is trained on the bulk U.S. sensitive personal data of U.S. persons. While not its primary commercial use, the chatbot is capable of reproducing or otherwise disclosing the bulk U.S. sensitive personal health data that was used to train the chatbot when responding to queries. The U.S. subsidiary knowingly licenses subscription-based access to that chatbot

worldwide, including to covered persons such as its parent entity. Although licensing use of the chatbot itself may not necessarily “involve access” to bulk U.S. sensitive personal data, the U.S. subsidiary knows or should know that the license can be used to obtain access to the U.S. persons’ bulk sensitive personal training data if prompted. The licensing of access to this bulk U.S. sensitive personal data is data brokerage because it involves the transfer of data from the U.S. company (*i.e.*, the provider) to licensees (*i.e.*, the recipients), where the recipients did not collect or process the data directly from the individuals linked or linkable to the collected or processed data. Even though the license did not explicitly provide access to the data, this is a prohibited transaction because the U.S. company knew or should have known that the use of the chatbot pursuant to the license could be used to obtain access to the training data, and because the U.S. company licensed the product to covered persons.

(2) [Reserved]

§ 202.302 Other prohibited data-brokerage transactions involving potential onward transfer to countries of concern or covered persons.

(a) *Prohibition.* Except as otherwise authorized pursuant to this part, no U.S. person, on or after the effective date, may knowingly engage in any transaction that involves any access by a foreign person to government-related data or bulk U.S. sensitive personal data and that involves data brokerage with any foreign person that is not a covered person unless the U.S. person:

(1) Contractually requires that the foreign person refrain from engaging in a subsequent covered data transaction involving data brokerage of the same data with a country of concern or covered person; and

(2) Reports any known or suspected violations of this contractual requirement in accordance with paragraph (b) of this section.

(b) *Reporting known or suspected violations—*(1) *When reports are due.* U.S. persons shall file reports within 14 days of the U.S. person becoming aware of a known or suspected violation.

(2) *Contents of reports.* Reports on known or suspected violations shall include the following, to the extent the information is known and available to the person filing the report at the time of the report:

(i) The name and address of the U.S. person reporting the known or suspected violation of the contractual requirement in accordance with paragraph (b) of this section;

(ii) A description of the known or suspected violation, including:

(A) Date of known or suspected violation;

(B) Description of the data-brokerage transaction referenced in paragraph (a) of this section;

(C) Description of the contractual provision prohibiting the onward transfer of the same data to a country of concern or covered person;

(D) Description of the known or suspected violation of the contractual obligation prohibiting the foreign person from engaging in a subsequent covered data transaction involving the same data with a country of concern or a covered person;

(E) Any persons substantively participating in the transaction referenced in paragraph (a) of this section;

(F) Information about the known or suspected persons involved in the onward data transfer transaction, including the name and location of any covered persons or countries of concern;

(G) A copy of any relevant documentation received or created in connection with the transaction; and

(iii) Any other information that the Department of Justice may require or any other information that the U.S. person filing the report believes to be pertinent to the known or suspected violation or the implicated covered person.

(3) *Additional contents; format and method of submission.* Reports required by this section must be submitted in accordance with this section and with subpart L of this part.

(c) *Examples—*(1) *Example 1.* A U.S. business knowingly enters into an agreement to sell bulk human genomic data to a European business that is not a covered person. The U.S. business is required to include in that agreement a

§ 202.303

28 CFR Ch. I (7-1-25 Edition)

limitation on the European business' right to resell or otherwise engage in a covered data transaction involving data brokerage of that data to a country of concern or covered person. Otherwise, the agreement would be a prohibited transaction.

(2) *Example 2.* A U.S. company owns and operates a mobile app for U.S. users with available advertising space. As part of selling the advertising space, the U.S. company provides the bulk precise geolocation data, IP address, and advertising IDs of its U.S. users' devices to an advertising exchange based in Europe that is not a covered person. The U.S. company's provision of this data to the advertising exchange is data brokerage and a prohibited transaction unless the U.S. company obtains a contractual commitment from the advertising exchange not to engage in any covered data transactions involving data brokerage of that same data with a country of concern or covered person.

(3) *Example 3.* A U.S. business knowingly enters into an agreement to buy bulk human genomic data from a European business that is not a covered person. This provision does not require the U.S. business to include any contractual limitation because the transaction does not involve access by the foreign person.

§ 202.303 Prohibited human 'omic data and human biospecimen transactions.

Except as otherwise authorized pursuant to this part, no U.S. person, on or after the effective date, may knowingly engage in any covered data transaction with a country of concern or covered person that involves access by that country of concern or covered person to bulk U.S. sensitive personal data that involves bulk human 'omic data, or to human biospecimens from which bulk human 'omic data could be derived.

§ 202.304 Prohibited evasions, attempts, causing violations, and conspiracies.

(a) *Prohibition.* Any transaction on or after the effective date that has the purpose of evading or avoiding, causes a violation of, or attempts to violate

any of the prohibitions set forth in this part is prohibited. Any conspiracy formed to violate the prohibitions set forth in this part is prohibited.

(b) *Examples—(1) Example 1.* A U.S. data broker seeks to sell bulk U.S. sensitive personal data to a foreign person who primarily resides in China. With knowledge that the foreign person is a covered person and with the intent to evade the regulations, the U.S. data broker invites the foreign person to travel to the United States to consummate the data transaction and transfer the bulk U.S. sensitive personal data in the United States. After completing the transaction, the person returns to China with the bulk U.S. sensitive personal data. The transaction in the United States is not a covered data transaction because the person who resides in China is a U.S. person while in the United States (unless that person was individually designated as a covered person pursuant to § 202.211(a)(5), in which case their covered person status would remain, even while in the United States, and the transaction would be a covered data transaction). However, the U.S. data broker has structured the transaction to evade the regulation's prohibitions on covered data transactions with covered persons. As a result, this transaction has the purpose of evading the regulations and is prohibited.

(2) *Example 2.* A Russian national, who is employed by a corporation headquartered in Russia, travels to the United States to conduct business with the Russian company's U.S. subsidiary, including with the purpose of obtaining bulk U.S. sensitive personal data from the U.S. subsidiary. The U.S. subsidiary is a U.S. person, the Russian corporation is a covered person, and the Russian employee is a covered person while outside the United States but a U.S. person while temporarily in the United States (unless that Russian employee was individually designated as a covered person pursuant to § 202.211(a)(5), in which case their covered person status would remain, even while in the United States, and the transaction would be a covered data transaction). With knowledge of these facts, the U.S. subsidiary licenses access to bulk U.S. sensitive personal

data to the Russian employee while in the United States, who then returns to Russia. This transaction has the purpose of evading the regulations and is prohibited.

(3) *Example 3.* A U.S. subsidiary of a company headquartered in a country of concern collects bulk precise geolocation data from U.S. persons. The U.S. subsidiary is a U.S. person, and the parent company is a covered person. With the purpose of evading the regulations, the U.S. subsidiary enters into a vendor agreement with a foreign company that is not a covered person. The vendor agreement provides the foreign company access to the data. The U.S. subsidiary knows (or reasonably should know) that the foreign company is a shell company, and knows that it subsequently outsources the vendor agreement to the U.S. subsidiary's parent company. This transaction has the purpose of evading the regulations and is prohibited.

(4) *Example 4.* A U.S. company collects bulk personal health data from U.S. persons. With the purpose of evading the regulations, the U.S. company enters into a vendor agreement with a foreign company that is not a covered person. The agreement provides the foreign company access to the data. The U.S. company knows (or reasonably should know) that the foreign company is a front company staffed primarily by covered persons. The U.S. company has not complied with either the security requirements in § 202.248 or other applicable requirements for conducting restricted transactions as detailed in subpart J of this part. This transaction has the purpose of evading the regulations and is prohibited.

(5) *Example 5.* A U.S. online gambling company uses an artificial intelligence algorithm to analyze collected bulk covered personal identifiers to identify users based on impulsivity for targeted advertising. The algorithm is trained on bulk covered personal identifiers and may reveal that raw data. A U.S. subsidiary of a company headquartered in a country of concern knows that the algorithm can reveal the training data. For the purpose of evasion, the U.S. subsidiary licenses the derivative algorithm from the U.S. online gambling company for the purpose of accessing

bulk sensitive personal identifiers from the training data that would not otherwise be accessible to the parent company and shares the algorithm with the parent company so that the parent company can obtain the bulk covered personal identifiers. The U.S. subsidiary's licensing transaction with the parent company has the purpose of evading the regulations and is prohibited.

§ 202.305 Knowingly directing prohibited or restricted transactions.

(a) *Prohibition.* Except as otherwise authorized pursuant to this part, no U.S. person, on or after the effective date, may knowingly direct any covered data transaction that would be a prohibited transaction or restricted transaction that fails to comply with the requirements of subpart D of this part and all other applicable requirements under this part, if engaged in by a U.S. person.

(b) *Examples—(1) Example 1.* A U.S. person is an officer, senior manager, or equivalent senior-level employee at a foreign company that is not a covered person, and the foreign company undertakes a covered data transaction at that U.S. person's direction or with that U.S. person's approval when the covered data transaction would be prohibited if performed by a U.S. person. The U.S. person has knowingly directed a prohibited transaction.

(2) *Example 2.* Several U.S. persons launch, own, and operate a foreign company that is not a covered person, and that foreign company, under the U.S. persons' operation, undertakes covered data transactions that would be prohibited if performed by a U.S. person. The U.S. persons have knowingly directed a prohibited transaction.

(3) *Example 3.* A U.S. person is employed at a U.S.-headquartered multinational company that has a foreign affiliate that is not a covered person. The U.S. person instructs the U.S. company's compliance unit to change (or approve changes to) the operating policies and procedures of the foreign affiliate with the specific purpose of allowing the foreign affiliate to undertake covered data transactions that would be prohibited if performed by a

§ 202.305

U.S. person. The U.S. person has knowingly directed prohibited transactions.

(4) *Example 4.* A U.S. bank processes a payment from a U.S. person to a covered person, or from a covered person to a U.S. person, as part of that U.S. person's engagement in a prohibited transaction. The U.S. bank has not knowingly directed a prohibited transaction, and its activity would not be prohibited (although the U.S. person's covered data transaction would be prohibited).

(5) *Example 5.* A U.S. financial institution underwrites a loan or otherwise provides financing for a foreign company that is not a covered person, and the foreign company undertakes covered data transactions that would be prohibited if performed by a U.S. person. The U.S. financial institution has not knowingly directed a prohibited transaction, and its activity would not be prohibited.

(6) *Example 6.* A U.S. person, who is employed at a foreign company that is not a covered person, signs paperwork approving the foreign company's procurement of real estate for its operations. The same foreign company separately conducts data transactions that use or are facilitated by operations at that real estate location and that would be prohibited transactions if performed by a U.S. person, but the U.S. employee has no role in approving or directing those separate data transactions. The U.S. person has not knowingly directed a prohibited transaction, and the U.S. person's activity would not be prohibited.

(7) *Example 7.* A U.S. company owns or operates a submarine telecommunications cable with one landing point in a foreign country that is not a country of concern and one landing point in a country of concern. The U.S. company leases capacity on the cable to U.S. customers that transmit bulk U.S. sensitive personal data to the landing point in the country of concern, including transmissions as part of prohibited transactions. The U.S. company's ownership or operation of the cable does not constitute knowingly directing a prohibited transaction, and its ownership or operation of the cable would not be prohibited (although the U.S.

28 CFR Ch. I (7-1-25 Edition)

customers' covered data transactions would be prohibited).

(8) *Example 8.* A U.S. person engages in a vendor agreement involving bulk U.S. sensitive personal data with a foreign person who is not a covered person. Such vendor agreement is not a restricted or prohibited transaction. The foreign person then employs an individual who is a covered person and grants them access to bulk U.S. sensitive personal data without the U.S. person's knowledge or direction. There is no covered data transaction between the U.S. person and the covered person, and there is no indication that the parties engaged in these transactions with the purpose of evading the regulations (such as the U.S. person having knowingly directed the foreign person's employment agreement with the covered person or the parties knowingly structuring a restricted transaction into these multiple transactions with the purpose of evading the prohibition). The U.S. person has not knowingly directed a restricted transaction.

(9) *Example 9.* A U.S. company sells DNA testing kits to U.S. consumers and maintains bulk human genomic data collected from those consumers. The U.S. company enters into a contract with a foreign cloud-computing company (which is not a covered person) to store the U.S. company's database of human genomic data. The foreign company hires employees from other countries, including citizens of countries of concern who primarily reside in a country of concern, to manage databases for its customers, including the U.S. company's human genomic database. There is no indication of evasion, such as the U.S. company knowingly directing the foreign company's employment agreements or the U.S. company knowingly engaging in and structuring these transactions to evade the regulations. The cloud-computing services agreement between the U.S. company and the foreign company would not be prohibited or restricted because that transaction is between a U.S. person and a foreign company that does not meet the definition of a covered person. The employment agreements between the foreign company and the covered persons would not be prohibited or restricted because those

agreements are between foreign persons.

Subpart D—Restricted Transactions**§ 202.401 Authorization to conduct restricted transactions.**

(a) *Restricted transactions.* Except as otherwise authorized pursuant to subparts E or H of this part or any other provision of this part, no U.S. person, on or after the effective date, may knowingly engage in a covered data transaction involving a vendor agreement, employment agreement, or investment agreement with a country of concern or covered person unless the U.S. person complies with the security requirements (as defined by § 202.248) required by this subpart D and all other applicable requirements under this part.

(b) This subpart D does not apply to covered data transactions involving access to bulk human genomic data or human biospecimens from which such data can be derived, and which are subject to the prohibition in § 202.303.

(c) *Examples*—(1) *Example 1.* A U.S. company engages in an employment agreement with a covered person to provide information technology support. As part of their employment, the covered person has access to personal financial data. The U.S. company implements and complies with the security requirements. The employment agreement is authorized as a restricted transaction because the company has complied with the security requirements.

(2) *Example 2.* A U.S. company engages in a vendor agreement with a covered person to store bulk personal health data. Instead of implementing the security requirements as identified by reference in this subpart D, the U.S. company implements different controls that it believes mitigate the covered person's access to the bulk personal health data. Because the U.S. person has not complied with the security requirements, the vendor agreement is not authorized and thus is a prohibited transaction.

(3) *Example 3.* A U.S. person engages in a vendor agreement involving bulk U.S. sensitive personal data with a foreign person who is not a covered person.

The foreign person then employs an individual who is a covered person and grants them access to bulk U.S. sensitive personal data without the U.S. person's knowledge or direction. There is no covered data transaction between the U.S. person and the covered person, and there is no indication that the parties engaged in these transactions with the purpose of evading the regulations (such as the U.S. person having knowingly directed the foreign person's employment agreement with the covered person or the parties knowingly structuring a prohibited transaction into these multiple transactions with the purpose of evading the prohibition). As a result, neither the vendor agreement nor the employment agreement would be a restricted transaction.

[90 FR 1706, Jan. 8, 2025, as amended at 90 FR 16466, Apr. 18, 2025]

§ 202.402 [Reserved]**Subpart E—Exempt Transactions****§ 202.501 Personal communications.**

This part does not apply to data transactions to the extent that they involve any postal, telegraphic, telephonic, or other personal communication that does not involve the transfer of anything of value.

§ 202.502 Information or informational materials.

This part does not apply to data transactions to the extent that they involve the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or informational materials.

§ 202.503 Travel.

This part does not apply to data transactions to the extent that they are ordinarily incident to travel to or from any country, including importation of accompanied baggage for personal use; maintenance within any country, including payment of living expenses and acquisition of goods or services for personal use; and arrangement or facilitation of such travel, including nonscheduled air, sea, or land voyages.

§ 202.504

28 CFR Ch. I (7-1-25 Edition)

§ 202.504 Official business of the United States Government.

(a) *Exemption.* Subparts C, and D, J, and K (other than § 202.1102 and § 202.1104) of this part do not apply to data transactions to the extent that they are for the conduct of the official business of the United States Government by its employees, grantees, or contractors; any authorized activity of any United States Government department or agency (including an activity that is performed by a Federal depository institution or credit union supervisory agency in the capacity of receiver or conservator); or transactions conducted pursuant to a grant, contract, or other agreement entered into with the United States Government.

(b) *Examples—*(1) *Example 1.* A U.S. hospital receives a Federal grant to conduct human genomic research on U.S. persons. As part of that federally funded human genomic research, the U.S. hospital contracts with a foreign laboratory that is a covered person, hires a researcher that is a covered person, and gives the laboratory and researcher access to the human biospecimens and human genomic data in bulk. The contract with the foreign laboratory and the employment of the researcher are exempt transactions but would be prohibited transactions if they were not part of the federally funded research.

(2) *Example 2.* A U.S. research institution receives a Federal grant to conduct human genomic research on U.S. and foreign persons. The Federal grant directs the U.S. research institution to publicize the results of its research, including the underlying human genomic data, via an internet-accessible database open to public health researchers with valid log-in credentials who pay a small annual fee to access the database, including covered persons primarily resident in a country of concern. The Federal grant does not cover the full costs of the authorized human genomic research or creation and publication of the database. The U.S. research institution obtains funds from private institutions and donors to fund the remaining costs. The human genomic research authorized by the Federal grant and publication of the database at the direction of the Fed-

eral grant would constitute a “transaction[] conducted pursuant to a grant, contract, or other agreement entered into with the United States Government.” The U.S. research institution must still comply with any requirements or prohibitions on sharing bulk U.S. sensitive personal data with countries of concern or covered persons required by the Federal grantmaker.

(3) *Example 3.* Same as Example 2, but the Federal grant is limited in scope to funding the U.S. research institution’s purchase of equipment needed to conduct the human genomic research and does not include funding related to publication of the data. The Federal grant does not direct or authorize the U.S. research institution to publicize the human genomic research or make it available to country of concern or covered person researchers via the database for which researchers pay an annual fee to access, or otherwise fund the conduct of the human genomic research. The U.S. research institution contracts with a foreign laboratory that is a covered person and gives the laboratory access to the bulk human genomic data. The contract with the foreign laboratory is not an exempt transaction because that transaction is not within the scope of the Federal grant.

§ 202.505 Financial services.

(a) *Exemption.* Subparts C, D, J, and K (other than § 202.1102 and § 202.1104) of this part do not apply to data transactions, to the extent that they are ordinarily incident to and part of the provision of financial services, including:

(1) Banking, capital-markets (including investment-management services as well as trading and underwriting of securities, commodities, and derivatives), or financial-insurance services;

(2) A financial activity authorized for national banks by 12 U.S.C. 24 (Seventh) and rules and regulations and written interpretations of the Office of the Comptroller of the Currency thereunder;

(3) An activity that is “financial in nature or incidental to such financial activity” or “complementary to a financial activity,” section (k)(1), as set forth in section (k)(4) of the Bank

Holding Company Act of 1956 (12 U.S.C. 1843(k)(4)) and rules and regulations and written interpretations of the Board of Governors of the Federal Reserve System thereunder;

(4) The transfer of personal financial data or covered personal identifiers incidental to the purchase and sale of goods and services (such as the purchase, sale, or transfer of consumer products and services through online shopping or e-commerce marketplaces);

(5) The provision or processing of payments or funds transfers (such as person-to-person, business-to-person, and government-to-person funds transfers) involving the transfer of personal financial data or covered personal identifiers, or the provision of services ancillary to processing payments and funds transfers (such as services for payment dispute resolution, payor authentication, tokenization, payment gateway, payment fraud detection, payment resiliency, mitigation and prevention, and payment-related loyalty point program administration); and

(6) The provision of investment-management services that manage or provide advice on investment portfolios or individual assets for compensation (such as devising strategies and handling financial assets and other investments for clients) or provide services ancillary to investment-management services (such as broker-dealers or futures commission merchants executing trades within an investment portfolio based upon instructions from an investment advisor).

(b) *Examples*—(1) *Example 1.* A U.S. company engages in a data transaction to transfer personal financial data in bulk to a financial institution that is incorporated in, located in, or subject to the jurisdiction or control of a country of concern to clear and settle electronic payment transactions between U.S. individuals and merchants in a country of concern where both the U.S. individuals and the merchants use the U.S. company's infrastructure, such as an e-commerce platform. Both the U.S. company's transaction transferring bulk personal financial data and the payment transactions by U.S. individuals are exempt transactions because

they involve access by a covered person to bulk personal financial data, but are ordinarily incident to and part of a financial service.

(2) *Example 2.* As ordinarily incident to and part of securitizing and selling asset-backed obligations (such as mortgage and nonmortgage loans) to a covered person, a U.S. bank provides bulk U.S. sensitive personal data to the covered person. The data transfers are exempt transactions because they involve access by a covered person to bulk personal financial data, but are ordinarily incident to and part of a financial service.

(3) *Example 3.* A U.S. bank or other financial institution, as ordinarily incident to and part of facilitating payments to U.S. persons in a country of concern, stores and processes the customers' bulk financial data using a data center operated by a third-party service provider in the country of concern. The use of this third-party service provider is a vendor agreement because it involves access by a covered person to personal financial data, but it is an exempt transaction that is ordinarily incident to and part of facilitating international payment.

(4) *Example 4.* Same as Example 3, but the underlying payments are between U.S. persons in the United States and do not involve a country of concern. The use of this third-party service provider is a vendor agreement, but it is not an exempt transaction because it involves access by a covered person to bulk personal financial data and it is not ordinarily incident to facilitating this type of financial activity.

(5) *Example 5.* As part of operating an online marketplace for the purchase and sale of goods, a U.S. company, as ordinarily incident to and part of U.S. consumers' purchase of goods on that marketplace, transfers bulk contact information, payment information (e.g., credit-card account number, expiration data, and security code), and delivery address to a merchant in a country of concern. The data transfers are exempt transactions because they involve access by a covered person to bulk personal financial data, but they are ordinarily incident to and part of U.S. consumers' purchase of goods.

§ 202.505

28 CFR Ch. I (7-1-25 Edition)

(6) *Example 6.* A U.S. investment adviser purchases securities of a company incorporated in a country of concern for the accounts of its clients. The investment adviser engages a broker-dealer located in a country of concern to execute the trade, and, as ordinarily incident to and part of the transaction, transfers to the broker-dealer its clients' covered personal identifiers and financial account numbers in bulk. This provision of data is an exempt transaction because it involves access by a covered person to bulk personal financial data, but it is ordinarily incident to and part of the provision of investment-management services.

(7) *Example 7.* A U.S. company that provides payment-processing services sells bulk U.S. sensitive personal data to a covered person. This sale is prohibited data brokerage and is not an exempt transaction because it involves access by a covered person to bulk personal financial data and is not ordinarily incident to and part of the payment-processing services provided by the U.S. company.

(8) *Example 8.* A U.S. bank facilitates international funds transfers to foreign persons not related to a country of concern, but through intermediaries or locations subject to the jurisdiction or control of a country of concern. These transfers result in access to bulk financial records by some covered persons to complete the transfers and manage associated risks. Providing this access as part of these transfers is ordinarily incident to the provision of financial services and is exempt.

(9) *Example 9.* A U.S. insurance company underwrites personal insurance to U.S. persons residing in foreign countries in the same region as a country of concern. The insurance company relies on its own business infrastructure and personnel in the country of concern to support its financial activity in the region, which results in access to the bulk U.S. sensitive personal data of some U.S.-person customers residing in the region, to covered persons at the insurance company supporting these activities. Providing this access is ordinarily incident to the provision of financial services and is exempt.

(10) *Example 10.* A U.S. financial services provider operates a foreign branch

in a country of concern and provides financial services to U.S. persons living within the country of concern. The financial services provider receives a lawful request from the regulator in the country of concern to review the financial activity conducted in the country, which includes providing access to the bulk U.S. sensitive personal data of U.S. persons resident in the country or U.S. persons conducting transactions through the foreign branch. The financial services provider is also subject to ongoing and routine reporting requirements from various regulators in the country of concern. Responding to the regulator's request, including providing access to this bulk U.S. sensitive personal data, is ordinarily incident to the provision of financial services and is exempt.

(11) *Example 11.* A U.S. bank voluntarily shares information, including relevant bulk U.S. sensitive personal data, with financial institutions organized under the laws of a country of concern for the purposes of, and consistent with industry practices for, fraud identification, combatting money laundering and terrorism financing, and U.S. sanctions compliance. Sharing this data for these purposes involves access by a covered person to bulk personal financial data, but is ordinarily incident to the provision of financial services and is exempt.

(12) *Example 12.* A U.S. company provides wealth-management services and collects bulk personal financial data on its U.S. clients. 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. In connection with the board's data security and cybersecurity responsibilities, the director could compel company personnel or influence company policies or practices to provide the director access to the underlying bulk personal financial data the company collects on its U.S. clients. The appointment of the director, who is a covered person, is a restricted employment agreement and is not exempt because the board member does not need to access, and in normal circumstances would not be able to access, the bulk financial data to perform his or her responsibilities. The board member's access to the bulk

personal financial data is not ordinarily incident to the U.S. company's provision of wealth-management services.

§ 202.506 Corporate group transactions.

(a) Subparts C, D, J, and K (other than § 202.1102 and § 202.1104) of this part do not apply to data transactions to the extent they are:

(1) Between a U.S. person and its subsidiary or affiliate located in (or otherwise subject to the ownership, direction, jurisdiction, or control of) a country of concern; and

(2) Ordinarily incident to and part of administrative or ancillary business operations, including:

(i) Human resources;

(ii) Payroll, expense monitoring and reimbursement, and other corporate financial activities;

(iii) Paying business taxes or fees;

(iv) Obtaining business permits or licenses;

(v) Sharing data with auditors and law firms for regulatory compliance;

(vi) Risk management;

(vii) Business-related travel;

(viii) Customer support;

(ix) Employee benefits; and

(x) Employees' internal and external communications.

(b) *Examples*—(1) *Example 1*. A U.S. company has a foreign subsidiary located in a country of concern, and the U.S. company's U.S.-person contractors perform services for the foreign subsidiary. As ordinarily incident to and part of the foreign subsidiary's payments to the U.S.-person contractors for those services, the U.S. company engages in a data transaction that gives the subsidiary access to the U.S.-person contractors' bulk personal financial data and covered personal identifiers. This is an exempt corporate group transaction.

(2) *Example 2*. A U.S. company aggregates bulk personal financial data. The U.S. company has a subsidiary that is a covered person because it is headquartered in a country of concern. The subsidiary is subject to the country of concern's national security laws requiring it to cooperate with and assist the country's intelligence services. The exemption for corporate group

transactions would not apply to the U.S. parent's grant of a license to the subsidiary to access the parent's databases containing the bulk personal financial data for the purpose of complying with a request or order by the country of concern under those national security laws to provide access to that data because granting of such a license is not ordinarily incident to and part of administrative or ancillary business operations.

(3) *Example 3*. A U.S. company's affiliate operates a manufacturing facility in a country of concern for one of the U.S. company's products. The affiliate uses employee fingerprints as part of security and identity verification to control access to that facility. To facilitate its U.S. employees' access to that facility as part of their job responsibilities, the U.S. company provides the fingerprints of those employees in bulk to its affiliate. The transaction is an exempt corporate group transaction.

(4) *Example 4*. A U.S. company has a foreign subsidiary located in a country of concern that conducts research and development for the U.S. company. The U.S. company sends bulk personal financial data to the subsidiary for the purpose of developing a financial software tool. The transaction is not an exempt corporate group transaction because it is not ordinarily incident to and part of administrative or ancillary business operations.

(5) *Example 5*. Same as Example 4, but the U.S. company has a foreign branch located in a country of concern instead of a foreign subsidiary. Because the foreign branch is a U.S. person as part of the U.S. company, the transaction occurs within the same U.S. person and is not subject to the prohibitions or restrictions. If the foreign branch allows employees who are covered persons to access the bulk personal financial data to develop the financial software tool, the foreign branch has engaged in restricted transactions.

(6) *Example 6*. A U.S. financial services provider has a subsidiary located in a country of concern. Customers of the U.S. company conduct financial transactions in the country of concern, and customers of the foreign subsidiary conduct financial transactions in the

§ 202.507

United States. To perform customer service functions related to these financial transactions, the foreign subsidiary accesses bulk U.S. sensitive personal data—specifically, personal financial data. The corporate group transactions exemption would apply to the foreign subsidiary's access to the personal financial data under these circumstances because it is ordinarily incident to and part of the provision of customer support. The foreign subsidiary's access to the personal financial data would also be covered by the financial services exemption.

§ 202.507 Transactions required or authorized by Federal law or international agreements, or necessary for compliance with Federal law.

(a) *Required or authorized by Federal law or international agreements.* Subparts C, D, J, and K (other than § 202.1102 and § 202.1104) of this part do not apply to data transactions to the extent they are required or authorized by Federal law or pursuant to an international agreement to which the United States is a party, including relevant provisions in the following:

(1) Annex 9 to the Convention on International Civil Aviation, International Civil Aviation Organization Doc. 7300 (2022);

(2) Section 2 of the Convention on Facilitation of International Maritime Traffic (1965);

(3) Articles 1, 12, 14, and 16 of the Postal Payment Services Agreement (2021);

(4) Articles 63, 64, and 65 of the Constitution of the World Health Organization (1946);

(5) Article 2 of the Agreement Between the Government of the United States of America and the Government of the People's Republic of China Regarding Mutual Assistance in Customs Matters (1999);

(6) Article 7 of the Agreement Between the Government of the United States of America and the Government of the People's Republic of China on Mutual Legal Assistance in Criminal Matters (2000);

(7) Article 25 of the Agreement Between the Government of the United States of America and the Government of the People's Republic of China for

the Avoidance of Double Taxation and the Prevention of Tax Evasion with Respect to Taxes on Income (1987);

(8) Article 2 of the Agreement Between the United States of America and the Macao Special Administrative Region of the People's Republic of China for Cooperation to Facilitate the Implementation of FATCA (2021);

(9) The Agreement between the Government of the United States and the Government of the People's Republic of China on Cooperation in Science and Technology (1979), as amended and extended;

(10) Articles II, III, VII of the Protocol to Extend and Amend the Agreement Between the Department of Health and Human Services of the United States of America and the National Health and Family Planning Commission of the People's Republic of China for Cooperation in the Science and Technology of Medicine and Public Health (2013);

(11) Article III of the Treaty Between the United States and Cuba for the Mutual Extradition of Fugitives from Justice (1905);

(12) Articles 3, 4, 5, 7 of the Agreement Between the Government of the United States of America and the Government of the Russian Federation on Cooperation and Mutual Assistance in Customs Matters (1994);

(13) Articles 1, 2, 5, 7, 13, and 16 of the Treaty Between the United States of America and the Russian Federation on Mutual Legal Assistance in Criminal Matters (1999);

(14) Articles I, IV, IX, XV, and XVI of the Treaty Between the Government of the United States of America and the Government of the Republic of Venezuela on Mutual Legal Assistance in Criminal Matters (1997); and

(15) Articles 5, 6, 7, 9, 11, 19, 35, and 45 of the International Health Regulations (2005).

(b) *Global health and pandemic preparedness.* Subparts C and D of this part do not apply to data transactions to the extent they are required or authorized by the following:

(1) The Pandemic Influenza Preparedness and Response Framework; and

(2) The Global Influenza Surveillance and Response System.

Department of Justice**§ 202.508**

(c) *Compliance with Federal law.* Subparts C and D of this part do not apply to data transactions to the extent that they are ordinarily incident to and part of ensuring compliance with any Federal laws and regulations, including the Bank Secrecy Act, 12 U.S.C. 1829b, 1951 through 1960, 31 U.S.C. 310, 5311 through 5314, 5316 through 5336; the Securities Act of 1933, 15 U.S.C. 77a *et seq.*; the Securities Exchange Act of 1934, 15 U.S.C. 78a *et seq.*; the Investment Company Act of 1940, 15 U.S.C. 80a-1 *et seq.*; the Investment Advisers Act of 1940, 15 U.S.C. 80b-1 *et seq.*; the International Emergency Economic Powers Act, 50 U.S.C. 1701 *et seq.*; the Export Administration Regulations, 15 CFR 730 *et seq.*; or any notes, guidance, orders, directives, or additional regulations related thereto.

(d) *Examples—(1) Example 1.* A U.S. bank or other financial institution engages in a covered data transaction with a covered person that is ordinarily incident to and part of ensuring compliance with U.S. laws and regulations (such as OFAC sanctions and anti-money laundering programs required by the Bank Secrecy Act). This is an exempt transaction.

(2) [Reserved]

§ 202.508 Investment agreements subject to a CFIUS action.

(a) *Exemption.* Subparts C, D, J, and K (other than § 202.1102 and § 202.1104) of this part do not apply to data transactions to the extent that they involve an investment agreement that is subject to a CFIUS action.

(b) *Examples—(1) Example 1.* A U.S. software provider is acquired in a CFIUS covered transaction by a foreign entity in which the transaction parties sign a mitigation agreement with CFIUS. The agreement has provisions governing the acquirer's ability to access the data of the U.S. software provider and their customers. The mitigation agreement contains a provision stating that it is a CFIUS action for purposes of this part. Before the effective date of the CFIUS mitigation agreement, the investment agreement is not subject to a CFIUS action and remains subject to these regulations to the extent otherwise applicable. Beginning on the effective date of the CFIUS

mitigation agreement, the investment agreement is subject to a CFIUS action and is exempt from this part.

(2) *Example 2.* Same as Example 1, but CFIUS issues an interim order before entering a mitigation agreement. The interim order states that it constitutes a CFIUS action for purposes of this part. Before the effective date of the interim order, the investment agreement is not subject to a CFIUS action and remains subject to these regulations to the extent otherwise applicable. Beginning on the effective date of the interim order, the investment agreement is subject to a CFIUS action and is exempt from this part. The mitigation agreement also states that it constitutes a CFIUS action for purposes of this part. After the effective date of the mitigation agreement, the investment agreement remains subject to a CFIUS action and is exempt from this part.

(3) *Example 3.* A U.S. biotechnology company is acquired by a foreign multinational corporation. CFIUS reviews this acquisition and concludes action without mitigation. This acquisition is not subject to a CFIUS action, and the acquisition remains subject to this part to the extent otherwise applicable.

(4) *Example 4.* A U.S. manufacturer is acquired by a foreign owner in which the transaction parties sign a mitigation agreement with CFIUS. The mitigation agreement provides for supply assurances and physical access restrictions but does not address data security, and it does not contain a provision explicitly designating that it is a CFIUS action. This acquisition is not subject to a CFIUS action, and the acquisition remains subject to this part to the extent otherwise applicable.

(5) *Example 5.* As a result of CFIUS's review and investigation of a U.S. human genomic company's acquisition by a foreign healthcare company, CFIUS refers the transaction to the President with a recommendation to require the foreign acquirer to divest its interest in the U.S. company. The President issues an order prohibiting the transaction and requiring divestment of the foreign healthcare company's interests and rights in the human genomic company. The presidential order itself does not constitute

§ 202.509

28 CFR Ch. I (7-1-25 Edition)

a CFIUS action. Unless CFIUS takes action, such as by entering into an agreement or imposing conditions to address risk prior to completion of the divestment, the transaction remains subject to this part to the extent otherwise applicable for as long as the investment agreement remains in existence following the presidential order and prior to divestment.

(6) *Example 6.* A U.S. healthcare company and foreign acquirer announce a transaction that they believe will be subject to CFIUS jurisdiction and disclose that they intend to file a joint voluntary notice soon. No CFIUS action has occurred yet, and the transaction remains subject to this part to the extent otherwise applicable.

(7) *Example 7.* Same as Example 6, but the transaction parties file a joint voluntary notice with CFIUS. No CFIUS action has occurred yet, and the transaction remains subject to this part to the extent otherwise applicable.

(8) *Example 8.* Company A, a covered person, acquires 100% of the equity and voting interest of Company B, a U.S. business that maintains bulk U.S. sensitive personal data of U.S. persons. After completing the transaction, the parties fail to implement the security requirements and other conditions required under this part. Company A and Company B later submit a joint voluntary notice to CFIUS with respect to the transaction. Upon accepting the notice, CFIUS determines that the transaction is a covered transaction and takes measures to mitigate interim risk that may arise as a result of the transaction until such time that the Committee has completed action, pursuant to 50 U.S.C. 4565(1)(3)(A)(iii). The interim order states that it constitutes a CFIUS action for purposes of this part. Beginning on the effective date of these measures imposed by the interim order, the security requirements and other applicable conditions under this part no longer apply to the transaction. The Department of Justice, however, may take enforcement action under this part, in coordination with CFIUS, with respect to the violations that occurred before the effective date of the interim order issued by CFIUS.

(9) *Example 9.* Same as Example 8, but before engaging in the investment agreement for the acquisition, Company A and Company B submit the joint voluntary notice to CFIUS. CFIUS determines that the transaction is a CFIUS covered transaction, CFIUS identifies a risk related to data security arising from the transaction, and CFIUS negotiates and enters into a mitigation agreement with the parties to resolve that risk. The mitigation agreement contains a provision stating that it is a CFIUS action for purposes of this part. Because a CFIUS action has occurred before the parties engage in the investment agreement, the acquisition is exempt from this part.

(10) *Example 10.* Same as Example 8, but before engaging in the investment agreement for the acquisition, the parties implement the security requirements and other conditions required under these regulations. Company A and Company B then submit a joint voluntary notice to CFIUS, which determines that the transaction is a CFIUS covered transaction. CFIUS identifies a risk related to data security arising from the transaction but determines that the regulations in this part adequately resolve the risk. CFIUS concludes action with respect to the transaction without taking any CFIUS action. Because no CFIUS action has occurred, the transaction remains subject to this part.

(11) *Example 11.* Same facts as Example 10, but CFIUS determines that the security requirements and other conditions applicable under this part are inadequate to resolve the national security risk identified by CFIUS. CFIUS negotiates a mitigation agreement with the parties to resolve the risk, which contains a provision stating that it is a CFIUS action for purposes of this part. The transaction is exempt from this part beginning on the effective date of the CFIUS mitigation agreement.

§ 202.509 Telecommunications services.

(a) *Exemption.* Subparts C, D, J, and K (other than § 202.1102 and § 202.1104) of this part do not apply to data transactions, other than those involving data brokerage, to the extent that they

are ordinarily incident to and part of the provision of telecommunications services.

(b) *Examples*—(1) *Example 1.* A U.S. telecommunications service provider collects covered personal identifiers from its U.S. subscribers. Some of those subscribers travel to a country of concern and use their mobile phone service under an international roaming agreement. The local telecommunications service provider in the country of concern shares these covered personal identifiers with the U.S. service provider for the purposes of either helping provision service to the U.S. subscriber or receiving payment for the U.S. subscriber's use of the country of concern service provider's network under that international roaming agreement. The U.S. service provider provides the country of concern service provider with network or device information for the purpose of provisioning services and obtaining payment for its subscribers' use of the local telecommunications service provider's network. Over the course of 12 months, the volume of network or device information shared by the U.S. service provider with the country of concern service provider for the purpose of provisioning services exceeds the applicable bulk threshold. These transfers of bulk U.S. sensitive personal data are ordinarily incident to and part of the provision of telecommunications services and are thus exempt transactions.

(2) *Example 2.* A U.S. telecommunications service provider collects precise geolocation data on its U.S. subscribers. The U.S. telecommunications service provider sells this precise geolocation data in bulk to a covered person for the purpose of targeted advertising. This sale is not ordinarily incident to and part of the provision of telecommunications services and remains a prohibited transaction.

§ 202.510 Drug, biological product, and medical device authorizations.

(a) *Exemption.* Except as specified in paragraph (a)(2) of this section, subparts C, D, J, and K (other than § 202.1102 and § 202.1104) of this part do not apply to a data transaction that

(1) Involves “regulatory approval data” as defined in paragraph (b) of this section and

(2) Is necessary to obtain or maintain regulatory authorization or approval to research or market a drug, biological product, device, or a combination product, provided that the U.S. person complies with the recordkeeping and reporting requirements set forth in §§ 202.1101(a) and 202.1102 with respect to such transaction.

(b) *Regulatory approval data.* For purposes of this section, the term *regulatory approval data* means sensitive personal data that is de-identified or pseudonymized consistent with the standards of 21 CFR 314.80 and that is required to be submitted to a regulatory entity, or is required by a regulatory entity to be submitted to a covered person, to obtain or maintain authorization or approval to research or market a drug, biological product, device, or combination product, including in relation to post-marketing studies and post-marketing product surveillance activities, and supplemental product applications for additional uses. The term excludes sensitive personal data not reasonably necessary for a regulatory entity to assess the safety and effectiveness of the drug, biological product, device, or combination product.

(c) *Other terms.* For purposes of this section, the terms “drug,” “biological product,” “device,” and “combination product” have the meanings given to them in 21 U.S.C. 321(g)(1), 42 U.S.C. 262(i)(1), 21 U.S.C. 321(h)(1), and 21 CFR 3.2(e), respectively.

(d) *Examples*—(1) *Example 1.* A U.S. pharmaceutical company seeks to market a new drug in a country of concern. The company submits a marketing application to the regulatory entity in the country of concern with authority to approve the drug in the country of concern. The marketing application includes the safety and effectiveness data reasonably necessary to obtain regulatory approval in that country. The transfer of data to the country of concern's regulatory entity is exempt from the prohibitions in this part.

(2) *Example 2.* Same as Example 1, except the regulatory entity in the country of concern requires that the data be

§ 202.511

de-anonymized. The transfer of data is not exempt under this section, because the data includes sensitive personal data that is identified to an individual.

(3) *Example 3.* Same as Example 1, except country of concern law requires foreign pharmaceutical companies to submit regulatory approval data using (1) a registered agent who primarily resides in the country of concern, (2) a country of concern incorporated subsidiary, or (3) an employee located in a country of concern. The U.S. pharmaceutical company enters into a vendor agreement with a registered agent in the country of concern to submit the regulatory approval data to the country of concern regulator. The U.S. pharmaceutical company provides to the registered agent only the regulatory approval data the U.S. pharmaceutical company intends the registered agent to submit to the country of concern regulator. The transaction with the registered agent is exempt, because it is necessary to obtain approval to market the drug in a country of concern. The U.S. pharmaceutical company must comply with the record-keeping and reporting requirements set forth in §§ 202.1101(a) and 202.1102 with respect to such transaction, however.

(4) *Example 4.* Same as Example 1, except the U.S. company enters a vendor agreement with a covered person located in the country of concern to store and organize the bulk U.S. sensitive personal data for eventual submission to the country of concern regulator. Country of concern law does not require foreign pharmaceutical companies to enter into such vendor agreements. The transaction is not exempt under this section, because the use of a covered person to store and organize the bulk U.S. sensitive personal data for the company's regulatory submission is not necessary to obtain regulatory approval.

(5) *Example 5.* A U.S. pharmaceutical company has obtained regulatory approval to market a new drug in a country of concern. The country of concern regulator requires the U.S. pharmaceutical company to submit de-identified sensitive personal data collected as part of the company's post-marketing product surveillance activities to assess the safety and efficacy of the

28 CFR Ch. I (7-1-25 Edition)

drug to the country of concern regulator via a country of concern registered agent to maintain the U.S. pharmaceutical company's authorization to market the drug. Sharing the de-identified sensitive personal data with the country of concern regulator via the country of concern registered agent to maintain marketing authorization is exempt from the prohibitions and restrictions in subparts C and D of this part.

(6) *Example 6.* A U.S. medical device manufacturer provides de-identified bulk U.S. personal health data to a country of concern regulator to obtain authorization to research the safety and effectiveness of a medical device in the country of concern. Country of concern law requires medical device manufacturers to conduct such safety research to obtain regulatory approval to market a new device. The prohibitions and restrictions of subparts C and D of this part do not apply to the de-identified regulatory approval data submitted to the country of concern regulator to obtain authorization to research the device's safety and effectiveness.

§ 202.511 Other clinical investigations and post-marketing surveillance data.

(a) *Exemption.* Subparts C, D, J, and K (other than § 202.1102 and § 202.1104) of this part do not apply to data transactions to the extent that those transactions are:

(1) Ordinarily incident to and part of clinical investigations regulated by the U.S. Food and Drug Administration ("FDA") under sections 505(i) and 520(g) of the Federal Food, Drug, and Cosmetic Act ("FD&C Act") or clinical investigations that support applications to the FDA for research or marketing permits for drugs, biological products, devices, combination products, or infant formula; or

(2) Ordinarily incident to and part of the collection or processing of clinical care data indicating real-world performance or safety of products, or the collection or processing of post-marketing surveillance data (including pharmacovigilance and post-marketing safety monitoring), and necessary to support or maintain authorization by

Department of Justice**§ 202.702**

the FDA, provided the data is de-identified or pseudonymized consistent with the standards of 21 CFR 314.80.

(b) *Other terms.* For purposes of this section, the terms “drug,” “biological product,” “device,” “combination product,” and “infant formula” have the meanings given to them in 21 U.S.C. 321(g)(1), 42 U.S.C. 262(i)(1), 21 U.S.C. 321(h)(1), 21 CFR 3.2(e), and 21 U.S.C. 321(z) respectively.

Subpart F—Determination of Countries of Concern**§ 202.601 Determination of countries of concern.**

(a) *Countries of concern.* Solely for purposes of the Order and this part, the Attorney General has determined, with the concurrence of the Secretaries of State and Commerce, that the following foreign governments have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of U.S. persons and pose a significant risk of exploiting government-related data or bulk U.S. sensitive personal data to the detriment of the national security of the United States or security and safety of U.S. persons:

- (1) China;
- (2) Cuba;
- (3) Iran;
- (4) North Korea;
- (5) Russia; and
- (6) Venezuela.

(b) *Effective date of amendments.* Any amendment to the list of countries of concern will apply to any covered data transaction that is initiated, pending, or completed on or after the effective date of the amendment.

Subpart G—Covered Persons**§ 202.701 Designation of covered persons.**

(a) *Designations.* The Attorney General may designate any person as a covered person for purposes of this part if, after consultation with the Department of State and any other agencies as the Attorney General deems appropriate, the Attorney General determines the person meets any of the cri-

teria set forth in § 202.211(a)(5) of this part.

(b) *Information considered.* In determining whether to designate a person as a covered person, the Attorney General may consider any information or material the Attorney General deems relevant and appropriate, classified or unclassified, from any Federal department or agency or from any other source.

(c) *Covered Persons List.* The names of persons designated as a covered person for purposes of this part, transactions with whom are prohibited or restricted pursuant to this part, are published in the **FEDERAL REGISTER** and incorporated into the National Security Division’s Covered Persons List. The Covered Persons List is accessible through the following page on the National Security Division’s website at <https://www.justice.gov/nsd>.

(d) *Non-exhaustive.* The list of designated covered persons described in this section is not exhaustive of all covered persons and supplements the categories in the definition of covered persons in § 202.211.

(e) *Effective date; actual and constructive knowledge.* (1) Designation as a covered person will be effective from the date of any public announcement by the Department. Except as otherwise authorized in this part, a U.S. person with actual knowledge of a designated person’s status is prohibited from knowingly engaging in a covered data transaction with that person on or after the date of the Department’s public announcement.

(2) Publication in the **FEDERAL REGISTER** is deemed to provide constructive knowledge of a person’s status as a covered person.

§ 202.702 Procedures governing removal from the Covered Persons List.

(a) *Requests for removal from the Covered Persons List.* A person may petition to seek administrative reconsideration of their designation, or may assert that the circumstances resulting in the designation no longer apply, and thus seek to be removed from the Covered Persons List pursuant to the following administrative procedures:

§ 202.801

28 CFR Ch. I (7-1-25 Edition)

(b) *Content of requests.* A covered person designated under paragraph (a) of this section may submit arguments or evidence that the person believes establish that insufficient basis exists for the designation. Such a person also may propose remedial steps on the person's part, such as corporate reorganization, resignation of persons from positions in a listed entity, or similar steps, that the person believes would negate the basis for designation.

(c) *Additional content; form and method of submission.* Requests for removal from the Covered Persons List must be submitted in accordance with this section and with subpart L of this part.

(d) *Requests for more information.* The information submitted by the listed person seeking removal will be reviewed by the Attorney General, who may request clarifying, corroborating, or other additional information.

(e) *Meetings.* A person seeking removal may request a meeting with the Attorney General; however, such meetings are not required, and the Attorney General may, in the Attorney General's discretion, decline to conduct such a meeting prior to completing a review pursuant to this section.

(f) *Decisions.* After the Attorney General has conducted a review of the request for removal, and after consultation with other agencies as the Attorney General deems appropriate, the Attorney General will provide a written decision to the person seeking removal. A covered person's status as a covered person—including its associated prohibitions and restrictions under this part—remains in effect during the pendency of any request to be removed from the Covered Persons List.

Subpart H—Licensing

§ 202.801 General licenses.

(a) *General course of procedure.* The Department may, as appropriate, issue general licenses to authorize, under appropriate terms and conditions, transactions that are subject to the prohibitions or restrictions in this part. In determining whether to issue a general license, the Attorney General may consider any information or material the Attorney General deems relevant and appropriate, classified or unclassified,

from any Federal department or agency or from any other source.

(b) *Relationship with specific licenses.* It is the policy of the Department not to grant applications for specific licenses authorizing transactions to which the provisions of a general license are applicable.

(c) *Reports.* Persons availing themselves of certain general licenses may be required to file reports and statements in accordance with the instructions specified in those licenses, this part or the Order. Failure to file timely all required information in such reports or statements may nullify the authorization otherwise provided by the general license and result in apparent violations of the applicable prohibitions that may be subject to enforcement action.

§ 202.802 Specific licenses.

(a) *General course of procedure.* Transactions subject to the prohibitions or restrictions in this part or the Order, and that are not otherwise permitted under this part or a general license, may be permitted only under a specific license, under appropriate terms and conditions.

(b) *Content of applications for specific licenses.* Applications for specific licenses shall include, at a minimum, a description of the nature of the transaction, including each of the following requirements:

(1) The types and volumes of government-related data or bulk U.S. sensitive personal data involved in the transactions;

(2) The identity of the transaction parties, including any ownership of entities or citizenship or primary residence of individuals;

(3) The end-use of the data and the method of data transfer; and

(4) Any other information that the Attorney General may require.

(c) *Additional content; form and method of submissions.* Requests for specific licenses must be submitted in accordance with this section and with subpart L of this part.

(d) *Additional conditions.* Applicants should submit only one copy of a specific license application to the Department; submitting multiple copies may result in processing delays. Any person

Department of Justice**§ 202.803**

having an interest in a transaction or proposed transaction may file an application for a specific license authorizing such a transaction.

(e) *Further information to be supplied.* Applicants may be required to furnish such further information as the Department deems necessary to assist in making a determination. Any applicant or other party-in-interest desiring to present additional information concerning a specific license application may do so at any time before or after the Department makes its decision with respect to the application. In unique circumstances, the Department may determine, in its discretion, that an oral presentation regarding a license application would assist in the Department's review of the issues involved. Any requests to make such an oral presentation must be submitted electronically by emailing the National Security Division at NSD.FIRS.datasecurity@usdoj.gov or using another official method to make such requests, in accordance with any instructions on the National Security Division's website.

(f) *Decisions.* In determining whether to issue a specific license, the Attorney General may consider any information or material the Attorney General deems relevant and appropriate, classified or unclassified, from any Federal department or agency or from any other source. The Department will advise each applicant of the decision respecting the applicant's filed application. The Department's decision with respect to a license application shall constitute final agency action.

(g) *Time to issuance.* The Department shall endeavor to respond to any request for a specific license within 45 days after receipt of the request and of any requested additional information and documents.

(h) *Scope.* (1) Unless otherwise specified in the license, a specific license authorizes the transaction:

(i) Only between the parties identified in the license;

(ii) Only with respect to the data described in the license; and

(iii) Only to the extent the conditions specified in the license are satisfied. The applicant must inform any other parties identified in the license of the

license's scope and of the specific conditions applicable to them.

(2) The Department will determine whether to grant specific licenses in reliance on representations the applicant made or submitted in connection with the license application, letters of explanation, and other documents submitted. Any license obtained based on a false or misleading representation in the license application, in any document submitted in connection with the license application, or during an oral presentation under this section shall be deemed void as of the date of issuance.

(i) *Reports under specific licenses.* As a condition for the issuance of any specific license, the licensee may be required to file reports or statements with respect to the transaction or transactions authorized by the specific license in such form and at such times as may be prescribed in the license. Failure to file timely all required information in such reports or statements may nullify the authorization otherwise provided by the specific license and result in apparent violations of the applicable prohibitions that may be subject to enforcement action.

(j) *Effect of denial.* The denial of a specific license does not preclude the reconsideration of an application or the filing of a further application. The applicant or any other party-in-interest may at any time request, by written correspondence, reconsideration of the denial of an application based on new facts or changed circumstances.

§ 202.803 General provisions.

(a) *Effect of license.* (1) No license issued under this subpart H, or otherwise issued by the Department, authorizes or validates any transaction effected prior to the issuance of such license or other authorization, unless specifically provided for in such license or authorization.

(2) No license issued under this subpart H authorizes or validates any transaction prohibited under or subject to this part unless the license is properly issued by the Department and specifically refers to this part.

(3) Any license authorizing or validating any transaction that is prohibited under or otherwise subject to this part has the effect of removing or

§ 202.901

28 CFR Ch. I (7-1-25 Edition)

amending those prohibitions or other requirements from the transaction, but only to the extent specifically stated by the terms of the license. Unless the license otherwise specifies, such an authorization does not create any right, duty, obligation, claim, or interest in, or with respect to, any property that would not otherwise exist under ordinary principles of law.

(4) Nothing contained in this part shall be construed to supersede the requirements established under any other provision of law or to relieve a person from any requirement to obtain a license or authorization from another department or agency of the United States Government in compliance with applicable laws and regulations subject to the jurisdiction of that department or agency. For example, issuance of a specific license authorizing a transaction otherwise prohibited by this part does not operate as a license or authorization to conclude the transaction that is otherwise required from the U.S. Department of Commerce, U.S. Department of State, U.S. Department of the Treasury, or any other department or agency of the United States Government.

(b) *Amendment, modification, or rescission.* Except as otherwise provided by law, any licenses (whether general or specific), authorizations, instructions, or forms issued thereunder may be amended, modified, or rescinded at any time.

(c) *Consultation.* The Department will issue, amend, modify, or rescind a general or specific license in concurrence with the Departments of State, Commerce, and Homeland Security and in consultation with other relevant agencies.

(d) *Exclusion from licenses and other authorizations.* The Attorney General reserves the right to exclude any person, property, or transaction from the operation of any license or from the privileges conferred by any license. The Attorney General also reserves the right to restrict the applicability of any license to particular persons, property, transactions, or classes thereof. Such actions are binding upon all persons receiving actual or constructive notice of the exclusions or restrictions.

Subpart I—Advisory Opinions

§ 202.901 Inquiries concerning application of this part.

(a) *General.* Any U.S. person party to a transaction potentially regulated under the Order and this part, or an agent of the party to such a transaction on the party's behalf, may request from the Attorney General a statement of the present enforcement intentions of the Department of Justice under the Order with respect to that transaction that may be subject to the prohibitions or restrictions in the Order and this part ("advisory opinion").

(b) *Anonymous, hypothetical, non-party and ex post facto review requests excluded.* The entire transaction that is the subject of the advisory opinion request must be an actual, as opposed to hypothetical, transaction and involve disclosed, as opposed to anonymous, parties to the transaction. Advisory opinion requests must be submitted by a U.S. person party to the transaction or that party's agent and have no application to a party that does not join the request. The transaction need not involve only prospective conduct, but an advisory opinion request will not be considered unless that portion of the transaction for which an opinion is sought involves only prospective conduct.

(c) *Contents.* Each advisory opinion request shall be specific and must be accompanied by all material information bearing on the conduct for which an advisory opinion is requested, and on the circumstances of the prospective conduct, including background information, complete copies of any and all operative documents, and detailed statements of all collateral or oral understandings, if any. Each request must include, at a minimum:

(1) The identities of the transaction parties, including any ownership of entities or citizenship or primary residence of individuals;

(2) A description of the nature of the transaction, including the types and volumes of government-related data or bulk U.S. sensitive personal data involved in the transaction, the end-use

Department of Justice**§ 202.901**

of the data, the method of data transfer, and any restrictions or requirements related to a party's right or ability to control, access, disseminate, or dispose of the data; and

(3) Any potential basis for exempting or excluding the transaction from the prohibitions or restrictions imposed in the Order and this part.

(d) *Additional contents; format and method of submissions.* Requests for advisory opinions must be submitted in accordance with this section and with subpart L of this part.

(e) *Further information to be supplied.* Each party shall provide any additional information or documents that the Department of Justice may thereafter request in its review of the matter. Any information furnished orally shall be confirmed promptly in writing; signed by or on behalf of the party that submitted the initial review request; and certified to be a true, correct, and complete disclosure of the requested information. A request will not be deemed complete until the Department of Justice receives such additional information. In connection with an advisory opinion request, the Department of Justice may conduct any independent investigation it believes appropriate.

(f) *Outcomes.* After submission of an advisory opinion request, the Department, in its discretion, may state its present enforcement intention under the Order and this part with respect to the proposed conduct; may decline to state its present enforcement intention; or, if circumstances warrant, may take such other position or initiate such other action as it considers appropriate. Any requesting party or parties may withdraw a request at any time prior to issuance of an advisory opinion. The Department remains free, however, to submit such comments to the requesting party or parties as it deems appropriate. Failure to take action after receipt of a request, documents, or information, whether submitted pursuant to this procedure or otherwise, shall not in any way limit or stop the Department from taking any action at such time thereafter as it deems appropriate. The Department reserves the right to retain any advisory opinion request, document, or informa-

tion submitted to it under this procedure or otherwise, to disclose any advisory opinion and advisory opinion request, including the identities of the requesting party and foreign parties to the transaction, the general nature and circumstances of the proposed conduct, and the action of the Department in response to any advisory opinion request, consistent with applicable law, and to use any such request, document, or information for any governmental purpose.

(g) *Time for response.* The Department shall endeavor to respond to any advisory opinion request within 30 days after receipt of the request and of any requested additional information and documents.

(h) *Written decisions only.* The requesting party or parties may rely only upon a written advisory opinion signed by the Attorney General.

(i) *Effect of advisory opinion.* Each advisory opinion can be relied upon by the requesting party or parties to the extent the disclosures made pursuant to this subpart I were accurate and complete and to the extent the disclosures continue accurately and completely to reflect circumstances after the date of the issuance of the advisory opinion. An advisory opinion will not restrict enforcement actions by any agency other than the Department of Justice. It will not affect a requesting party's obligations to any other agency or under any statutory or regulatory provision other than those specifically discussed in the advisory opinion.

(j) *Amendment or revocation of advisory opinion.* An advisory opinion may be amended or revoked at any time after it has been issued. Notice of such will be given in the same manner as notice of the advisory opinion was originally given or in the FEDERAL REGISTER. Whenever possible, a notice of amendment or revocation will state when the Department will consider a party's reliance on the superseded advisory opinion to be unreasonable, and any transition period that may be applicable.

(k) *Compliance.* Neither the submission of an advisory opinion request, nor its pendency, shall in any way alter the responsibility or obligation of a requesting party to comply with the

§ 202.1001

Order, this part, or any other applicable law.

Subpart J—Due Diligence and Audit Requirements

§ 202.1001 Due diligence for restricted transactions.

(a) *Data compliance program.* By no later than October 6, 2025, U.S. persons engaging in any restricted transactions shall develop and implement a data compliance program.

(b) *Requirements.* The data compliance program shall include, at a minimum, each of the following requirements:

(1) Risk-based procedures for verifying data flows involved in any restricted transaction, including procedures to verify and log, in an auditable manner, the following:

(i) The types and volumes of government-related data or bulk U.S. sensitive personal data involved in the transaction;

(ii) The identity of the transaction parties, including any ownership of entities or citizenship or primary residence of individuals; and

(iii) The end-use of the data and the method of data transfer;

(2) For restricted transactions that involve vendors, risk-based procedures for verifying the identity of vendors;

(3) A written policy that describes the data compliance program and that is annually certified by an officer, executive, or other employee responsible for compliance;

(4) A written policy that describes the implementation of the security requirements as defined in § 202.248 and that is annually certified by an officer, executive, or other employee responsible for compliance; and

(5) Any other information that the Attorney General may require.

§ 202.1002 Audits for restricted transactions.

(a) *Audit required.* U.S. persons that, on or after October 6, 2025, engage in any restricted transactions under § 202.401 shall conduct an audit that complies with the requirements of this section.

(b) *Who may conduct the audit.* The auditor:

28 CFR Ch. I (7-1-25 Edition)

(1) Must be qualified and competent to examine, verify, and attest to the U.S. person's compliance with and the effectiveness of the security requirements, as defined in § 202.248, and all other applicable requirements, as defined in § 202.401, implemented for restricted transactions;

(2) Must be independent; and

(3) Cannot be a covered person or a country of concern.

(c) *When required.* The audit must be performed once for each calendar year in which the U.S. person engages in any restricted transactions.

(d) *Timeframe.* The audit must cover the preceding 12 months.

(e) *Scope.* The audit must:

(1) Examine the U.S. person's restricted transactions;

(2) Examine the U.S. person's data compliance program required under § 202.1001 and its implementation;

(3) Examine relevant records required under § 202.1101;

(4) Examine the U.S. person's security requirements, as defined by § 202.248; and

(5) Use a reliable methodology to conduct the audit.

(f) *Report.* (1) The auditor must prepare and submit a written report to the U.S. person within 60 days of the completion of the audit.

(2) The audit report must:

(i) Describe the nature of any restricted transactions engaged in by the U.S. person;

(ii) Describe the methodology undertaken, including the relevant policies and other documents reviewed, relevant personnel interviewed, and any relevant facilities, equipment, networks, or systems examined;

(iii) Describe the effectiveness of the U.S. person's data compliance program and its implementation;

(iv) Describe any vulnerabilities or deficiencies in the implementation of the security requirements that have affected or could affect the risk of access to government-related data or bulk U.S. sensitive personal data by a country of concern or covered person;

(v) Describe any instances in which the security requirements failed or

Department of Justice**§ 202.1102**

were otherwise not effective in mitigating the risk of access to government-related data or bulk U.S. sensitive personal data by a country of concern or covered person; and

(vi) Recommend any improvements or changes to policies, practices, or other aspects of the U.S. person's business to ensure compliance with the security requirements.

(3) U.S. persons engaged in restricted transactions must retain the audit report for a period of at least 10 years, consistent with the recordkeeping requirements in § 202.1101.

Subpart K—Reporting and Recordkeeping Requirements**§ 202.1101 Records and recordkeeping requirements.**

(a) *Records.* Except as otherwise provided, U.S. persons engaging in any transaction subject to the provisions of this part shall keep a full and accurate record of each such transaction engaged in, and such record shall be available for examination for at least 10 years after the date of such transaction.

(b) *Additional recordkeeping requirements.* U.S. persons engaging in any restricted transaction shall create and maintain, at a minimum, the following records in an auditable manner:

(1) A written policy that describes the data compliance program and that is certified annually by an officer, executive, or other employee responsible for compliance;

(2) A written policy that describes the implementation of any applicable security requirements as defined in § 202.248 and that is certified annually by an officer, executive, or other employee responsible for compliance;

(3) The results of any annual audits that verify the U.S. person's compliance with the security requirements and any conditions on a license;

(4) Documentation of the due diligence conducted to verify the data flow involved in any restricted transaction, including:

(i) The types and volumes of government-related data or bulk U.S. sensitive personal data involved in the transaction;

(ii) The identity of the transaction parties, including any direct and indirect ownership of entities or citizenship or primary residence of individuals; and

(iii) A description of the end-use of the data;

(5) Documentation of the method of data transfer;

(6) Documentation of the dates the transaction began and ended;

(7) Copies of any agreements associated with the transaction;

(8) Copies of any relevant licenses or advisory opinions;

(9) The document reference number for any original document issued by the Attorney General, such as a license or advisory opinion;

(10) A copy of any relevant documentation received or created in connection with the transaction; and

(11) An annual certification by an officer, executive, or other employee responsible for compliance of the completeness and accuracy of the records documenting due diligence.

§ 202.1102 Reports to be furnished on demand.

(a) *Reports.* Every person is required to furnish under oath, in the form of reports or otherwise, from time to time and at any time as may be required by the Department of Justice, complete information relative to any act or transaction or covered data transaction, regardless of whether such act, transaction, or covered data transaction is effected pursuant to a license or otherwise, subject to the provisions of this part and except as otherwise prohibited by Federal law. The Department of Justice may require that such reports include the production of any books, contracts, letters, papers, or other hard copy or electronic documents relating to any such act, transaction, or covered data transaction, in the custody or control of the persons required to make such reports. Reports may be required either before, during, or after such acts, transactions, or covered data transactions. The Department of Justice may, through any person or agency, conduct investigations, hold hearings, administer oaths, examine witnesses, receive evidence, take depositions, and require by subpoena

§ 202.1103

28 CFR Ch. I (7-1-25 Edition)

the attendance and testimony of witnesses and the production of any books, contracts, letters, papers, and other hard copy or electronic documents relating to any matter under investigation, regardless of whether any report has been required or filed in connection therewith.

(b) *Definition of the term “document.”* For purposes of paragraph (a) of this section, the term *document* includes any written, recorded, or graphic matter or other means of preserving thought or expression (including in electronic format), and all tangible things stored in any medium from which information can be processed, transcribed, or obtained directly or indirectly, including correspondence, memoranda, notes, messages, contemporaneous communications such as text and instant messages, letters, emails, spreadsheets, metadata, contracts, bulletins, diaries, chronological data, minutes, books, reports, examinations, charts, ledgers, books of account, invoices, air waybills, bills of lading, worksheets, receipts, printouts, papers, schedules, affidavits, presentations, transcripts, surveys, graphic representations of any kind, drawings, photographs, graphs, video or sound recordings, and motion pictures or other film.

(c) *Format.* Persons providing documents to the Department of Justice pursuant to this section must produce documents in a usable format agreed upon by the Department of Justice. For guidance, see the Department of Justice’s data delivery standards available on the National Security Division’s website at <https://www.justice.gov/nsd>.

§ 202.1103 Annual reports.

(a) *Who must report.* An annual report must be filed, except as otherwise prohibited by Federal law, by any U.S. person that, on or after October 6, 2025, is engaged in a restricted transaction involving cloud-computing services, and that has 25% or more of the U.S. person’s equity interests owned (directly or indirectly, through any contract, arrangement, understanding, relationship, or otherwise) by a country of concern or covered person.

(b) *Primary responsibility to report.* A report may be filed on behalf of a U.S. person engaging in the data transaction described in § 202.1103(a) by an attorney, agent, or other person. Primary responsibility for reporting, however, rests with the actual U.S. person engaging in the data transaction. No U.S. person is excused from filing a report by reason of the fact that another U.S. person has submitted a report with regard to the same data transaction, except where the U.S. person has actual knowledge that the other U.S. person filed the report.

(c) *When reports are due.* A report on the data transactions described in § 202.1103(a) engaged in as of December 31 of the previous year shall be filed annually by March 1 of the subsequent year.

(d) *Contents of reports.* Annual reports on the data transactions described in § 202.1103(a) shall include the following:

(1) The name and address of the U.S. person engaging in the covered data transaction, and the name, telephone number, and email address of a contact from whom additional information may be obtained;

(2) A description of the covered data transaction, including:

(i) The date of the transaction;

(ii) The types and volumes of government-related data or bulk U.S. sensitive personal data involved in the transaction;

(iii) The method of data transfer; and

(iv) Any persons participating in the data transaction and their respective locations, including the name and location of each data recipient, the ownership of entities or citizenship or primary residence of individuals, the name and location of any covered persons involved in the transaction, and the name of any countries of concern involved in the transaction;

(3) A copy of any relevant documentation received or created in connection with the transaction; and

(4) Any other information that the Department of Justice may require.

(e) *Additional contents; format and method of submission.* Reports required by this section must be submitted in accordance with this section and with subpart L of this part.

Department of Justice**§ 202.1201****§ 202.1104 Reports on rejected prohibited transactions.**

(a) *Who must report.* A report must be filed, except as otherwise prohibited by Federal law, by any U.S. person that, on or after October 6, 2025, has received and affirmatively rejected (including automatically rejected using software, technology, or automated tools) an offer from another person to engage in a prohibited transaction involving data brokerage.

(b) *When reports are due.* U.S. persons shall file reports within 14 days of rejecting a transaction prohibited by this part.

(c) *Contents of reports.* Reports on rejected transactions shall include the following, to the extent known and available to the person filing the report at the time the transaction is rejected:

(1) The name and address of the U.S. person that rejected the prohibited transaction, and the name, telephone number, and email address of a contact from whom additional information may be obtained;

(2) A description of the rejected transaction, including:

(i) The date the transaction was rejected;

(ii) The types and volumes of government-related data or bulk U.S. sensitive personal data involved in the transaction;

(iii) The method of data transfer;

(iv) Any persons attempting to participate in the transaction and their respective locations, including the name and location of each data recipient, the ownership of entities or citizenship or primary residence of individuals, the name and location of any covered persons involved in the transaction, and the name of any countries of concern involved in the transaction;

(v) A copy of any relevant documentation received or created in connection with the transaction; and

(vi) Any other information that the Department of Justice may require.

(d) *Additional contents; format and method of submission.* Reports required by this section must be submitted in accordance with this section and with subpart L of this part.

Subpart L—Submitting Applications, Requests, Reports, and Responses**§ 202.1201 Procedures.**

(a) *Application of this subpart.* This subpart L applies to any submissions required or permitted by this part, including reports of known or suspected violations submitted pursuant to § 202.302, requests for removal from the Covered Persons List submitted pursuant to subpart G of this part, requests for specific licenses submitted pursuant to § 202.802, advisory opinion requests submitted pursuant to subpart I of this part, annual reports submitted pursuant to § 202.1103, reports on rejected prohibited transactions submitted pursuant to § 202.1104, and responses to pre-penalty notices and findings of violations submitted pursuant to § 202.1306 (collectively, “submissions”).

(b) *Form of submissions.* Submissions must follow the instructions in this part and any instructions on the National Security Division’s website. With the exception of responses to pre-penalty notices or findings of violations submitted pursuant to subpart M of this part, submissions must use the forms on the National Security Division’s website or another official reporting option as specified by the National Security Division.

(c) *Method of submissions.* Submissions must be made to the National Security Division electronically by emailing the National Security Division at NSD.FIRS.datasecurity@usdoj.gov or using another official electronic reporting option, in accordance with any instructions on the National Security Division’s website.

(d) *Certification.* If the submitting party is an individual, the submission must be signed by the individual or the individual’s attorney. If the submitting party is not an individual, the submission must be signed on behalf of each submitting party by an officer, director, a person performing the functions of an officer or a director of, or an attorney for, the submitting party. Annual reports submitted pursuant to § 202.1103, and reports on rejected transactions submitted pursuant to

§ 202.1301

§ 202.1104, must be signed by an officer, a director, a person performing the functions of an officer or a director, or an employee responsible for compliance. In appropriate cases, the Department of Justice may require the chief executive officer of a requesting party to sign the request. Each such person signing a submission must certify that the submission is true, accurate, and complete.

Subpart M—Penalties and Finding of Violation

§ 202.1301 Penalties for violations.

(a) *Civil and criminal penalties.* Section 206 of IEEPA, 50 U.S.C. 1705, is applicable to violations of the provisions of any license, ruling, regulation, order, directive, or instruction issued by or pursuant to the direction or authorization of the Attorney General pursuant to this part or otherwise under IEEPA.

(1) A civil penalty not to exceed the amount set forth in section 206 of IEEPA may be imposed on any person who violates, attempts to violate, conspires to violate, or causes a violation of any license, order, regulation, or prohibition issued under IEEPA.

(2) IEEPA provides for a maximum civil penalty not to exceed the greater of \$368,136 or an amount that is twice the amount of the transaction that is the basis of the violation with respect to which the penalty is imposed.

(3) A person who willfully commits, willfully attempts to commit, willfully conspires to commit, or aids or abets in the commission of a violation of any license, order, regulation, or prohibition issued under IEEPA shall, upon conviction, be fined not more than \$1,000,000, or if a natural person, may be imprisoned for not more than 20 years, or both.

(b) *Adjustment of civil penalties.* The civil penalties provided in IEEPA are subject to adjustment pursuant to the Federal Civil Penalties Inflation Adjustment Act of 1990 (Public Law 101-410, as amended, 28 U.S.C. 2461 note).

(c) *Adjustment of criminal penalties.* The criminal penalties provided in IEEPA are subject to adjustment pursuant to 18 U.S.C. 3571.

28 CFR Ch. I (7-1-25 Edition)

(d) *False statements.* Pursuant to 18 U.S.C. 1001, whoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully falsifies, conceals, or covers up by any trick, scheme, or device a material fact; or makes any materially false, fictitious, or fraudulent statement or representation; or makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry shall be fined under title 18, United States Code, imprisoned, or both.

(e) *Other applicable laws.* Violations of this part may also be subject to other applicable laws.

§ 202.1302 Process for pre-penalty notice.

(a) *When and how issued.* (1) If the Department of Justice has reason to believe that there has occurred a violation of any provision of this part or a violation of the provisions of any license, ruling, regulation, order, directive, or instruction issued by or pursuant to the direction or authorization of the Attorney General pursuant to this part or otherwise under IEEPA and determines that a civil monetary penalty is warranted, the Department of Justice will issue a pre-penalty notice informing the alleged violator of the agency's intent to impose a monetary penalty.

(2) The pre-penalty notice shall be in writing.

(3) The pre-penalty notice may be issued whether or not another agency has taken any action with respect to the matter.

(4) The Department shall provide the alleged violator with the relevant information that is not privileged, classified, or otherwise protected, and that forms the basis for the pre-penalty notice, including a description of the alleged violation and proposed penalty amount.

(b) *Opportunity to respond.* An alleged violator has the right to respond to a pre-penalty notice in accordance with § 202.1306.

(c) *Settlement.* Settlement discussion may be initiated by the Department of

Department of Justice**§ 202.1305**

Justice, the alleged violator, or the alleged violator's authorized representative.

(d) *Representation.* A representative of the alleged violator may act on behalf of the alleged violator, but any oral communication with the Department of Justice prior to a written submission regarding the specific allegations contained in the pre-penalty notice must be preceded by a written letter of representation, unless the pre-penalty notice was served upon the alleged violator in care of the representative.

§ 202.1303 Penalty imposition.

If, after considering any written response to the pre-penalty notice and any relevant facts, the Department of Justice determines that there was a violation by the alleged violator named in the pre-penalty notice and that a civil monetary penalty is appropriate, the Department of Justice may issue a penalty notice to the violator containing a determination of the violation and the imposition of the monetary penalty. The Department shall provide the violator with any relevant, non-classified information that forms the basis of the penalty. The issuance of the penalty notice shall constitute final agency action. The violator has the right to seek judicial review of that final agency action in Federal district court.

§ 202.1304 Administrative collection and litigation.

In the event that the violator does not pay the penalty imposed pursuant to this part or make payment arrangements acceptable to the Department of Justice, the Department of Justice may refer the matter to the Department of the Treasury for administrative collection measures or take appropriate action to recover the penalty in any civil suit in Federal district court.

§ 202.1305 Finding of violation.

(a) *When and how issued.* (1) The Department of Justice may issue an initial finding of violation that identifies a violation if the Department of Justice:

(i) Determines that there has occurred a violation of any provision of this part, or a violation of the provi-

sions of any license, ruling, regulation, order, directive, or instruction issued by or pursuant to the direction or authorization of the Attorney General pursuant to this part or otherwise under IEEPA;

(ii) Considers it important to document the occurrence of a violation; and

(iii) Concludes that an administrative response is warranted but that a civil monetary penalty is not the most appropriate response.

(2) An initial finding of violation shall be in writing and may be issued whether or not another agency has taken any action with respect to the matter.

(3) The Department shall provide the alleged violator with the relevant information that is not privileged, classified, or otherwise protected, that forms the basis for the finding of violation, including a description of the alleged violation.

(b) *Opportunity to respond.* An alleged violator has the right to contest an initial finding of violation in accordance with § 202.1306.

(c) *Determination—(1) Determination that a finding of violation is warranted.* If, after considering the response, the Department of Justice determines that a final finding of violation should be issued, the Department of Justice will issue a final finding of violation that will inform the violator of its decision. The Department shall provide the violator with the relevant information that is not privileged, classified, or otherwise protected, that forms the basis for the finding of violation. A final finding of violation shall constitute final agency action. The violator has the right to seek judicial review of that final agency action in Federal district court.

(2) *Determination that a finding of violation is not warranted.* If, after considering the response, the Department of Justice determines a finding of violation is not warranted, then the Department of Justice will inform the alleged violator of its decision not to issue a final finding of violation. A determination by the Department of Justice that a final finding of violation is not warranted does not preclude the Department of Justice from pursuing other enforcement actions.

§ 202.1306

(d) *Representation.* A representative of the alleged violator may act on behalf of the alleged violator, but any oral communication with the Department of Justice prior to a written submission regarding the specific alleged violations contained in the initial finding of violation must be preceded by a written letter of representation, unless the initial finding of violation was served upon the alleged violator in care of the representative.

§ 202.1306 Opportunity to respond to a pre-penalty notice or finding of violation.

(a) *Right to respond.* An alleged violator has the right to respond to a pre-penalty notice or finding of violation by making a written presentation to the Department of Justice.

(b) *Deadline for response.* A response to a pre-penalty notice or finding of violation must be electronically submitted within 30 days of electronic service of the notice or finding. The failure to submit a response within 30 days shall be deemed to be a waiver of the right to respond.

28 CFR Ch. I (7-1-25 Edition)

(c) *Extensions of time for response.* Any extensions of time will be granted, at the discretion of the Department of Justice, only upon specific request to the Department of Justice.

(d) *Contents of response.* Any response should set forth in detail why the alleged violator either believes that a violation of the regulations did not occur or why a finding of violation or penalty is otherwise unwarranted under the circumstances. The response should include all documentary or other evidence available to the alleged violator that supports the arguments set forth in the response. The Department of Justice will consider all relevant materials submitted in the response.

Subpart N—Government-Related Location Data List**§ 202.1401 Government-Related Location Data List.**

For each Area ID listed in this section, each of the latitude/longitude coordinate pairs forms a corner of the geofenced area.

Department of Justice

§ 202.1401

TABLE 1 TO § 202.1401

Area ID		Latitude/longitude coordinates of geofenced areas
1	38.935624, -77.207888	38.931674, -77.199347 38.952077, -77.120947 38.953174, -77.369764 38.953174, -77.369759
2	38.950446, -77.125592	38.947468, -77.120060 38.951148, -77.369759
3	38.955191, -77.327792	38.951148, -77.369759
4	39.113546, -76.777053	39.100086, -76.749715 39.131086, -76.758527
5	33.416299, -82.172772	33.406350, -82.163645 33.416666, -82.184366
6	21.525083, -158.019139	21.518161, -158.012233 21.525362, -158.012364
7	21.475012, -158.061844	21.479226, -158.049881 21.483357, -158.057568
8	29.449322, -98.646174	29.452827, -98.637623 29.458967, -98.637623
9	39.2173162771, -76.362684384	39.2173162771, -76.362684384 39.5089896774, -76.362684384
10	39.040211182001, -76.968096219999	39.040211182001, -76.968096219999 39.040211182001, -76.968096219999
11	20.7457155230001, -156.440726997	20.7457155230001, -156.440726997 20.749410490001, -156.431116699
12	38.8805363480001, -77.109020989999	38.8811994730001, -77.109020989999 32.7862928992, -97.460085871
13	32.765632877, -97.460085871	32.7862928992, -97.460085871 34.62177924, -118.126219217
14	34.62177924, -118.126219217	34.62177924, -118.126219217 32.053229630001, -110.959444035
15	32.0505440380001, -84.50445929	32.053229630001, -110.959444035 33.9994487500001, -84.50445929
16	33.9994487500001, -84.50445929	33.9994487500001, -84.50445929 36.665761500001, -76.163567934
17	36.665761500001, -76.163567934	36.665761500001, -76.163567934 27.9157840450001, -98.061583281
18	27.9157840450001, -98.061583281	27.9157840450001, -98.061583281 21.37009858780001, -157.926772605
19	21.3545896960001, -157.926772605	21.37009858780001, -157.926772605 39.566862548, -78.871120656
20	39.528701323, -78.871120656	39.566862548, -78.871120656 31.235020282, -85.654625655
21	31.227908115, -85.654625655	31.235020282, -85.654625655 45.097292940001, -45.097292940001
22	45.097292940001, -83.5785134019999	45.097292940001, -83.5785134019999 -83.5785134019999, -99.303633301
23	34.637909800001, -117.126359987	34.637909800001, -117.126359987 32.6375106470001, -117.126359987
24	32.6375106470001, -117.126359987	32.6375106470001, -117.126359987 32.66985251, -117.12532209
25	32.66985251, -117.12532209	32.675675827, -117.172352209 13.5479750120001, -144.846656045
26	13.5479750120001, -144.846656045	13.6479724930001, -144.846656045 33.61019973, -86.013461889
27	33.61019973, -86.013461889	33.61019973, -86.013461889 27.6776476860001, -81.364060357
28	27.632285040001, -81.364060357	27.6776476860001, -81.364060357 38.86919115, -77.079135005
29	38.86919115, -77.079135005	38.86919115, -77.079135005 30.269654889, -77.081320445
30	30.269654889, -77.081320445	30.269654889, -77.081320445 28.585882605, -81.197868843
31	28.585882605, -81.197868843	28.585882605, -81.197868843 35.9939531130001, -35.9939531280001
32	35.9939531130001, -35.9939531280001	35.9939531280001, -35.9939531280001 -78.8988567119999, -78.8988567119999
33	-78.8988567119999, -78.8988567119999	-78.8988567119999, -78.8988567119999 35.448152643, -35.448152643
34	35.290688975, -74.486379079	35.290688975, -74.486379079 39.668741192, -74.486379079
35	39.668741192, -74.486379079	39.668741192, -74.486379079 27.5433418430001, -81.140127987
36	27.5433418430001, -81.140127987	27.5433418430001, -81.140127987 34.328662741, -89.704814972
37	34.328662741, -89.704814972	34.328662741, -89.704814972 32.730432780001, -117.142819245
38	32.7313462890001, -117.1427436521	32.7313462890001, -117.1427436521 44.824436067, -68.845190583
39	44.824436067, -68.845190583	44.824436067, -68.845190583 30.406043932, -87.651017989
40	30.406043932, -87.651017989	30.406043932, -87.651017989 30.378935891, -87.616693181

§ 202.1401

28 CFR Ch. I (7-1-25 Edition)

TABLE 1 TO § 202.1401—Continued

Area ID	Latitude/longitude coordinates of geofenced areas	
41	32.460689648, -93.692932035	32.533707929, -93.531044113
42	42.1637744650001, -72.721474954	42.1737587120001, -72.721474954
43	32.234848137, -114.563241999	32.74030565, -114.563241999
44	32.7717587880001, -112.742209944	32.9055316810001, -112.742209944
45	70.118081036, -143.64942567	70.13677672, -143.64942567
46	39.0718274430001, -121.477278056	39.1737524000001, -121.477278056
47	21.3446919420001, -157.715961149	21.3801950850001, -157.715961149
48	39.320337941, -80.2723884	39.332652421, -80.2723884
49	64.3151851490001, -146.65232338	64.320265380001, -146.65232338
50	33.564586567, -86.7593074919999	33.577571506, -86.7593074919999
51	33.979025715, -77.920042096	33.98353888, -77.920042096
52	37.6569067660001, -84.2697493589999	37.7403075720001, -84.2697493589999
53	43.549701982, -116.23995646	43.565222364, -116.23995646
54	41.928384165, -72.706470888	41.940084236, -72.706470888
55	41.5939882100001, -81.628180911	41.5451316070001, -81.628180911
56	38.253480861, -119.65128069	38.488443466, -119.65128069
57	32.7116821270001, -73.17842204	32.7116821270001, -73.17842204
58	40.5796208200001, -73.881158344	40.5851822330001, -73.881158344
59	31.3815422060001, -85.978073125	31.3915251500001, -85.978073125
60	39.6792307960001, -104.791155246	39.7256386980001, -104.791155246
61	44.465375824, -73.1658772108	44.481431105, -73.1658772108
62	18.2464477936, -65.580288041	18.250653732, -65.580288041
63	31.2653802660001, -85.701212602	31.29007820001, -85.701212602
64	13.488847714, 144.8237902	13.650804937, 144.8237902
65	41.613354353, -93.9831494479999	42.134619451, -93.9831494479999
66	34.619016640001, -84.1105367119999	34.635761430001, -84.0950752379999
67	44.5103232180001, -85.072276169999	44.897605610001, -84.4513643499999
68	35.0011406840001, -79.523939868	35.0683094360001, -79.442653881
69	32.641816536, -116.466773316	32.70380767, -116.466773316
70	32.70751941, -116.520980841	32.714794633, -116.520980841
71	35.1488975340001, -111.913136629	35.2519317510001, -111.913136629
72	35.688234998, -120.85951023	35.8893098334, -120.85951023
73	30.91049165, 89.245591473	31.215207751, 89.245591473
74	40.3878151230001, -112.116737638	40.4646164020001, -112.116737638
75	34.40563345, -103.337070541	34.412489823, -103.337070541
76	34.3614483640001, -103.354726446	34.4053770780001, -103.354726446
77	28.410283461, -80.611521457	28.5692329286, -80.611521457
78	58.6207566940001, -162.088477025	58.6671382160001, -162.05195173
79	39.843911672, -89.67315301	39.853707959, -89.664434939
80	40.199855450001, -77.1813079679999	40.199855450001, -77.1567188819999

81	48.720965666, -97.91415126	48.732224729, -97.91415126	48.732224729, -97.91415126	48.720965666, -97.892530954
82	30.3652267820001, -89.145003244	30.3839136300001, -89.145003244	30.3839136300001, -89.145003244	30.3652267820001, -89.10296884419999.
83	34.13152274, -119.113804625	34.1468546850001, -119.113804625	34.1468546850001, -119.107499465	34.13152274, -119.107499465
84	35.2130798550001, -80.93434288	35.2209434880001, -80.93434288	35.2209434880001, -80.924747233	35.2130798550001, -80.924747233
85	37.265469865, -76.649783157999	37.300168225, -76.649783157999	37.300168225, -76.649783157999	37.265469865, -76.649783157999.
86	38.652772446, -76.537514883	38.665190459, -76.537514883	38.665190459, -76.526755785	38.665190459, -76.526755785
87	38.730266928, -104.864157079	38.748479779, -104.864157079	38.748479779, -104.830998169	38.730266928, -104.830998169.
88	41.1558081, -104.827282882	41.163962628, -104.827282882	41.163962628, -104.811585256	41.163962628, -104.811585256
89	33.0433918000001, -115.769002927	33.561860554, -115.769002927	33.561860554, -114.937048224	33.0433918000001, -114.937048224.
90	64.256987909, -149.271311872	64.318532807, -149.271311872	64.318532807, -149.078725257	64.256987909, -149.078725257
91	48.018154470001, -122.74958066	48.0862406420001, -122.74958066	48.0862406420001, -122.699833714	48.018154470001, -122.699833714.
92	55.262639599, -162.88200844	55.262639599, -162.88200844	55.262639599, -162.882133146	55.262639599, -162.882133146.
93	32.9228514580001, -88.597781493	33.66113396510001, -88.597781493	33.66113396510001, -88.419408536	32.9228514580001, -88.419408536.
94	42.2857517910001, -71.386797532	42.2934966590001, -71.386797532	42.2934966590001, -71.355575286	42.2934966590001, -71.355575286.
95	30.396985159, -87.301358539	30.41034727, -87.301358539	30.41034727, -87.2728142462	30.396985159, -87.2728142462.
96	36.883299270001,	36.8838686090001,	36.8838686090001,	36.883299270001,
97	36.4941214200001, -115.88042321	36.7385429400001, -115.88042321	36.7385429400001, -115.88042321	36.4941214200001, -115.4868387
98	21.298764438, -158.073065748	21.327294536, -158.073065748	21.327294536, -158.044610628	21.298764438, -158.044610628
99	36.779547069, -119.702471155	36.782091919, -119.702471155	36.782091919, -119.701514522	36.779547069, -119.701514522.
100	42.15583814, -70.937475414999	42.158515225, -70.937475414999	42.158515225, -70.930174133999	42.158515225, -70.930174133999.
101	48.421495020001, -117.41300542	48.51515751880001, -117.41300542	48.51515751880001, -117.35926532	48.421495020001, -117.35926532.
102	26.091587869, -80.11918708	26.092840186, -80.11918708	26.092840186, -80.106205835	26.092840186, -80.106205835.
103	35.6459372400001, -75.981669019	35.7768890170001, -75.991669019	35.7768890170001, -75.771632698	35.6459372400001, -75.771632698.
104	32.1193109110001, -110.909314221	32.1962087390001, -110.78976372	32.1962087390001, -110.78976372.	32.1193109110001, -110.78976372.
105	37.408487004, -77.453738162	37.439266805, -77.453738162	37.439266805, -77.435618651	37.408487004, -77.435618651.
106	38.8781919000001, -77.109040482	38.87292949460001, -77.109040482	38.87292949460001, -77.108174294	38.87292949460001, -77.108174294.
107	40.1972506380001, -76.853865245	40.2226551520001, -76.853865245	40.2226551520001, -76.853865245	40.1972506380001, -76.853865245
108	39.974582163, -82.913383443	39.985122185, -82.913383443	39.985122185, -82.913383443	39.985122185, -82.913383443
109	41.537901628, -93.6474402705	41.549978514, -93.674278745	41.549978514, -93.674278745	41.537901628, -93.674278745.
110	30.40946552, -86.500613385	30.412738745, -86.500613385	30.412738745, -86.497174479999	30.40946552, -86.497174479999.
111	37.9630717110001, -122.027819871	38.0227201040001, -122.027819871	38.0227201040001, -121.1939142028	37.9630717110001, -121.1939142028.
112	39.8839370650001, -75.19093843	40.526695230001, -82.036414938	40.526695230001, -82.036414938	39.8839370650001, -75.16306509
113	42.491491200001, -83.909314383	42.5026695230001, -82.036414938	42.5026695230001, -82.036414938	42.491491200001, -83.037544269.
114	42.463482900001, -71.691664547	42.5765892500001, -71.691664547	42.5765892500001, -71.691664547	42.463482900001, -71.691664547
115	46.9314271700001, -67.896907739999	46.932671660001, -67.896907739999	46.932671660001, -67.896907739999	46.9314271700001, -67.896907739999.
116	21.567863645, -158.21347981	21.581592585, -158.21347981	21.581592585, -158.21347981	21.567863645, -158.21347981
117	28.067154520001, -98.778173769	28.1245884970001, -98.778173769	28.1245884970001, -98.778173769	28.067154520001, -98.778173769
118	33.8969244250001, -84.542380856	33.9367578460001, -84.542380856	33.9367578460001, -84.49530955	33.8969244250001, -84.49530955.
119	39.10596555, -75.494449085	39.152386899, -75.494449085	39.152386899, -75.436634728	39.10596555, -75.436634728.
120	24.568031467, -81.781745689	24.585123807, -81.781745689	24.585123807, -81.765170818	24.568031467, -81.765170818.
121	32.6743233394, -117.133765	32.692839739, -117.133765	32.692839739, -117.108967938	32.6743233394, -117.108967938.
122	46.83044210001, -92.21102751	46.8510308170001, -92.21102751	46.8510308170001, -92.165423416	46.83044210001, -92.165423416.
123	32.3941914100001, -99.867572545	32.4478988670001, -99.867572545	32.4478988670001, -99.808678428	32.3941914100001, -99.808678428.
124	52.704712400001, -174.053643507	52.7410254930001, -174.053643507	52.7410254930001, -174.15651898	52.70471240001, -174.15651898.
125	35.017611389, -117.140763438	35.017611389, -117.140763438	35.017611389, -117.140763438	34.762486344, -117.525081645.
126	30.381138945, -86.8509824239999	30.405275435, -86.8509824239999	30.405275435, -86.8509824239999	30.381138945, -86.6331687359999.

§ 202.1401

28 CFR Ch. I (7-1-25 Edition)

TABLE 1 TO § 202.1401—Continued

Area ID		Latitude/longitude coordinates of geofenced areas		
127	30.6217855130001, -86.75545942799999,	30.6494843350001, -86.75545942799999, 30.74917294690001, -86.983116121 30.7480079510001, -147.165786418 36.8708429060001, -76.334377989989,	30.6494843350001, -86.73037157599999, 30.7497294690001, -82.448862506 64.7480079510001, -146.938371648 36.8708429060001, -76.32987931199999, 29.6230511860001, -95.17474779 44.176511165, -103.129144564 31.34466339, -92.549004972 39.4140000010001, -77.9854 47.6428480860001, -117.693058242 39.942237, -117.125199131 36.9225983950001, -76.324596591 36.9206436430001, -76.324596591 24.567441214, -81.801443736 38.9672269860001, -95.68666717799999, 32.7263297590001, -117.225651967 41.4772592890001, -71.34288412999999, 38.6728683430001, -77.202015081 39.85326909, -86.028620872 31.7883139250001, -106.581474459 18.4221096420001, -66.13417534999999, 36.535433810001, -87.820914236 38.418237328, -104.967064928 30.7215072860001, -97.913021062 21.277988357, -157.837039889 39.426602934, -77.4374741934 39.02058900001, -77.080066807 39.0320227980001, -77.04385429 44.010913031, -75.842125669 33.27451935, -82.379611728 33.6096833770001, -84.35154274 63.9388112670001, -145.772613518 37.213516805, -77.358595158 40.604582683, -74.034049003 31.434363842, -110.449131361 35.793592310001, -121.426498813 35.6227078795, -117.084005937 34.0836392030001, -86.959251815 33.9829769470001, -80.704124579	30.6217855130001, -86.73037157599999, 27.0764966720001, -82.448862506 64.6012802210001, -146.938371648 36.8644398160001, -76.32987931199999, 29.5899224830001, -95.16633921 44.11298756, -103.0606660125 31.3525926945, -92.532050872 39.4012000000001, -77.9708 47.5887747180001, -117.62308229 33.3291382400001, -117.249241913 38.826363587, -117.125199131 36.9206436430001, -76.321048116 36.406669179, -81.613437212 24.567441214, -81.79382837 38.955509150001, -95.67399748999999, 32.7323348500001, -117.215769817 41.4772592890001, -71.34288412999999, 38.6728683430001, -77.12097347799999, 39.85326909, -86.003845091 32.6965880790001, -105.524846042 18.4221096420001, -66.15489820999999, 37.7288240330001, -87.423400866 38.765149865, -104.7820914236 38.765149865, -104.7820914236 38.765149865, -104.7820914236 38.765149865, -104.7820914236 31.392195710001, -97.38260936 21.28553417, -157.831141168 39.450390568, -77.410819037 38.021291415900001, -77.05003399 39.0346693610001, -77.03866628 44.256536804, -75.842125669 33.440619771, -82.379611728 33.6319158920001, -84.35154274 64.0231026060001, -145.772613518 63.9388112670001, -145.655809936 37.213516805, -77.358595158 40.613167841, -74.034049003 31.6866589773, -110.188946087 36.1147194860001, -121.03460619 35.6227078795, -117.084005937 34.0836392030001, -86.959251815 33.9829769470001, -80.704124579

Department of Justice

§ 202.1401

165	30.921870988, -93.579998793	31.490503162, -92.862745164	30.921870988, -92.862745164.
166	37.78807672, -86.056877114	38.0073711200001, -86.056877114	37.78807672, -86.747574551.
167	39.3284266340001, -94.949264706	39.32842663280001, -94.949264706	39.3284266340001, -94.880745646.
168	37.603763470001,	37.799972520001,	37.6037963470001,
	-92.2500513099999,	-92.0408380759999,	-92.0408380759999.
169	35.03462073, -79.380629689	35.2474563988, -79.380629689	35.03462073, -78.1901879671.
170	43.90284867, -90.765375865	44.159824233, -90.765375865	43.90284867, -90.587856875.
171	39.071479147, -76.776616336	39.130981819, -76.776616336	39.071479147, -76.79922204.
172	40.284497280001, -76.096750839	40.339052010001, -76.096750839	40.284497280001, -74.026249284.
173	37.00265414, -76.3170219039999	37.035192566, -76.3170219039999	37.00265414, -76.2925912168999.
174	32.2387118990001, -85.021200904	32.5517604030001, -84.637054935	37.00265414, -76.2925912168999.
175	31.37144049, -85.865695846	31.505687537, -85.865695846	37.00265414, -76.12193512.
176	39.036899860001, -96.962729439	39.3067854380001, -96.962729439	37.00265414, -76.12193512.
177	21.3344869650001, -157.894073145	21.3570876230001, -157.894073145	37.00265414, -76.12193512.
178	42.20346973, -87.8100502569999	42.216029281, -87.8100502569999	37.00265414, -76.12193512.
179	34.63759073, -98.755961597	34.768015017, -98.755961597	37.00265414, -76.12193512.
180	35.247127112, -94.37404048025	35.345197662, -94.37404048025	37.00265414, -76.12193512.
181	31.849045500001, -81.889008935	32.1248422650001, -81.889008935	37.00265414, -76.12193512.
182	63.495426454, -148.632607873	64.877948104, -148.652607873	37.00265414, -76.12193512.
183	38.018142733, -77.395132849	38.2229469870001, -77.395132849	37.00265414, -76.12193512.
184	35.225141090001, -108.629517745	35.523401050001, -108.629517745	37.00265414, -76.12193512.
185	66.552440738, -145.217198219	66.5628635721, -145.217198219	37.00265414, -76.12193512.
186	41.13159597, -104.888175803	41.20151583, -104.888175803	37.00265414, -76.12193512.
187	40.831716890001, -72.646569509	40.840459060001, -72.646569509	37.00265414, -76.12193512.
188	36.7632210320001, -119.768492626	36.7866408030001, -119.768492626	37.00265414, -76.12193512.
189	39.046072102, -76.689705918	39.068505337, -76.689705918	37.00265414, -76.12193512.
190	42.937147850001, -87.891735557	42.9447299110001, -87.891735557	37.00265414, -76.12193512.
191	40.653985350001, -89.713436026	40.671317760001, -89.713436026	37.00265414, -76.12193512.
192	42.297663631, -87.85623196999	42.303204758, -87.85623196999	37.00265414, -76.12193512.
193	42.0902179130001, -87.841261049999	42.0929537750001, -87.841261049999	37.00265414, -76.12193512.
194	31.410361906, -96.4658208399999	31.419467447, -96.4658208399999	37.00265414, -76.12193512.
195	33.422394339, -112.0056889	33.427659719, -112.015046889	37.00265414, -76.12193512.
196	31.42115244990001, -100.421423136	31.45029361800001, -100.421423136	37.00265414, -76.12193512.
197	41.53550126800001,	41.53983549900001,	37.00265414, -76.12193512.
	-71.3460647429999,	-71.3460647429999,	37.00265414, -76.12193512.
198	47.921152756, -97.423874209999	48.00111753, -97.423874209999	47.921152756, -97.423874209999.
199	32.73787564700001, -96.962007531	32.74213265200001, -96.962007531	32.73787564700001, -96.962007531.
200	47.471916874, -111.37032141	47.482136373, -111.37032141	47.471916874, -111.37032141.
201	38.935411516, -110.143618375	38.983389468, -110.143618375	38.935411516, -110.143618375.
202	40.62983635, -86.175582897	40.6784136910001, -86.175582897	40.62983635, -86.175582897.
203	30.404753499, -89.06446994	30.416012997, -89.06446994	30.404753499, -89.06446994.
204	62.384524694, -145.202752458	62.438701327, -145.202752458	62.384524694, -145.202752458.
205	43.0985253500001,	43.120405300001,	43.0985253500001.
	-76.1175710329999,	-76.1175710329999,	-76.1175710329999.
206	42.449141119, -71.292232959999	42.477596104, -71.292232959999	42.449141119, -71.292232959999.
207	32.728744878, -117.20895019	32.730100028, -117.20895019	32.728744878, -117.20895019.
208	44.220153461, -90.1171781241	44.249174018, -90.1171781241	44.220153461, -90.1171781241.
209	38.225497861, -118.850468214	38.675823329, -118.850468214	38.225497861, -118.850468214.
210	46.9082501180001, -96.813335915	46.9192707510001, -96.813335915	46.9082501180001, -96.813335915.

§ 202.1401

28 CFR Ch. I (7-1-25 Edition)

TABLE 1 TO § 202.1401—Continued

Area ID	Latitude/longitude coordinates of geofenced areas	
211	21.530784666, -158.026158574	21.541312201, -158.026158574
212	21.4521601660001, -158.036473816	21.45806965550001, -158.036473816
213	31.1479145100001, -85.744240415	31.1546432720001, -85.744240415
214	41.098339530001, -112.024398889	41.1651189630001, -112.024398889
215	32.793022870001, -106.204383402	33.0771883510001, -106.204383402
216	36.4958650500001, -82.684986348	36.5518898770001, -82.684986348
217	32.828679521, -115.288498013	32.846906967, -115.288498013
218	25.4901310200001,	25.5181528940001,
219	-80.4045291039999,	-80.4045291039999,
220	39.446631245, -87.304009056	39.458106621, -87.304009056
221	31.3751890450001,	31.3850761720001,
222	-85.5828701299999,	-85.5828701299999,
223	31.983269490001, -81.198805141	32.0349005460001, -81.198805141
224	30.406119645, -86.74211065	30.45486409, -86.74211065
225	32.5545394160001, -117.13305356	32.5724338440001, -117.13305356
226	65.964785140001, -153.812691683	66.1009998220001, -153.812691683
227	38.435308005, -85.627248303	38.4686353, -85.627248303
228	226.751643250, -91.325065862	240.751643250, -91.325065862
229	32.311624454, -90.0879237459999	32.328439256, -90.0879237459999
230	30.40257215, -81.628884649	30.408229141, -81.628884649
231	29.95708177420001, -81.972797144	30.49211986090001, -81.972797144
232	38.8109873670001,	39.0601368300001,
233	-85.4822157569999,	-85.4822157569999,
234	48.1670840830001, -121.958243024	48.1670840830001, -121.958243024
235	43.570013340001,	43.5962111540001,
236	-96.7051566289999,	-96.7051566289999,
237	38.823559833, -77.026428621	38.823559833, -77.026428621
238	38.7822985190001, -76.90343143	38.8289021577, -76.90343143
239	41.637293940001,	41.7708974620001,
240	-70.5993199659999,	-70.5993199659999,
241	32.873792982, -81.104787366	33.621879898, -81.104787366
242	61.1317682310001, -149.879980832	61.14090492570001, -149.879980832
243	37.063373746, -76.627940713	37.182586341, -76.627940713
244	45.8002376150001, -122.802079191	47.2187487550001, -122.802079191
245	39.944386000001, -74.66112648	40.0586108630001, -74.66112648
246	38.8803051040001, -77.084491842	38.8803051040001, -77.084491842
247	21.6863899190001, -158.1782288	21.6863899190001, -158.1782288
248	29.346205018, -98.690398725	29.8933089967, -98.690398725
249	36.982714836, -76.1925524759999	36.982892732, -76.1925524759999
250	37.8190118270001, -75.514689614	37.9512715100001, -75.514689614
251	40.7085310680001, -84.148196529	40.7086310680001, -84.148196529
252	41.373633960001, -88.082958084	41.373633960001, -88.082958084
253	41.4365859010001, -88.187831293	41.4365859010001, -88.187831293

Department of Justice

§ 202.1401

249	21.560298564, -158.266932035	21.572360392, -158.237835914	21.560298554, -158.237835914
250	21.02739240001, -158.035515202	21.6936355750001, -158.035515202	21.6936355750001, -157.95298888
251	22.042080758, -159.75916373	22.042080758, -159.75916373	22.042080758, -159.75916373
252	20.0291620130001, -155.834320072	20.0374297880001, -155.834320072	20.0374297880001, -155.823440805
253	30.398192666, -98.950868469999	30.420139346, -98.950868469999	30.420139346, -98.950868469999
254	36.7153178120001, -98.128361282	36.7154718519001, -98.128361282	36.7154718519001, -98.110051089
255	60.55873366, -151.257835285	60.560759837, -151.257835285	60.560759837, -151.254274297
256	19.4318712580001, -155.22720251	19.4367646340001, -155.22720251	19.4367646340001, -155.271614951
257	58.638365343, -156.693447262	58.638365343, -156.693447262	58.638365343, -156.45918473
258	42.144655070001, -121.753628091	42.1707914760001, -121.753628091	42.1707914760001, -121.727677654
259	21.4148860290001, -158.014284187	21.4580033840001, -158.014284187	21.4580033840001, -157.991853913
260	35.0873284870001, -106.513226109	35.0873284870001, -106.513226109	34.947171320001, -106.36076837
261	57.816468609, -152.341066882	57.826019097, -152.341066882	57.816468609, -152.325036589
262	66.837046801, -162.617184378	66.856648663, -162.617184378	66.856648663, -162.565302627
263	36.905846763, -76.304089839	36.905846763, -76.304089839	36.905846763, -76.300769409
264	39.080371583, -94.283657449	39.111476783, -94.283657449	39.111476783, -94.21198472
265	38.0785775570001, -92.611906773999	38.0962204240001, -92.611906773999	38.0962204240001, -92.598910347999
266	29.1056384770001, -100.811107299	29.3792559920001, -100.811107299	29.3792559920001, -100.460775759
267	39.975011278, -77.766381881	40.061676766, -77.766381881	40.061676766, -77.627738092
268	40.367062390001, -96.759207222	40.367062390001, -96.759207222	40.367062390001, -96.74825231
269	68.865164727, -166.153805131	68.877996761, -166.153805131	68.877996761, -166.053355378
270	34.881841514, -92.178032909	34.928710282, -92.178032909	34.928710282, -92.097368909
271	33.740760199001, -118.234788427	33.75147550001, -118.234788427	33.74517650001, -118.232155662
272	32.646434739, -94.170119305	32.6543891651, -94.170119305	32.6543891651, -94.10955796
273	33.916514003, -118.44928679	34.057048416, -118.44928679	34.057048416, -118.378717014
274	33.9581476250001, -118.23660337	33.95893839490001, -118.23660337	33.95893839490001, -118.235052573
275	38.173835389, -85.727224249999	38.181490413, -85.727224249999	38.181490413, -85.7200947549999
276	31.812802193, -85.654704728	31.818371904, -85.6546082241	31.818371904, -85.646082241
277	18.439120568, -65.997012649999	18.446763986, -65.997012649999	18.446763986, -65.98773319999
278	33.5136616280001, -112.545349748	33.724140570001, -112.545349748	33.724140570001, -112.319683167
279	27.821277441, -82.5260369709999	27.869304053, -82.5260369709999	27.869304053, -82.469154309
280	22.127046405, -159.721450962	22.13630275, -159.721450962	22.13630275, -159.71827724
281	21.5127546910001, -152.739749591	21.55147060001, -152.739749591	21.55147060001, -152.739919199
282	47.4870471620001, -111.1562151	47.5233762890001, -111.1562151	47.4870471620001, -111.152194907
283	47.562267324, -122.556511461	47.570404986, -122.556511461	47.570404986, -122.531291341
284	40.86209200001, -82.5260369709999	40.8156897690001, -82.5260369709999	40.8156897690001, -82.50961146
285	33.855508925, -117.319151995	33.916474996, -117.319151995	33.916474996, -116.984937475
286	34.2011154190001, -116.717969816	34.7339793100001, -116.717969816	34.7339793100001, -115.720717569
287	32.280961146, -80.76567248	32.510825603, -80.76567248	32.510825603, -80.65947492
288	34.6814644040001, -77.2633324639999	35.076192102, -77.2633324639999	35.076192102, -76.3302441279999
289	-77.276334639999	-72.902651119, -117.188623475	-72.902651119, -116.984937219
290	32.853111095, -117.188623475	34.746048414, -77.48420569999	34.746048414, -77.370277147
291	34.558215246, -82.50961146	32.679820865, -114.64004722	32.679820865, -114.578207704
292	34.4950770080001, -77.6073096539999	34.7485511280001, -77.177756721	34.4950770080001, -77.177756721
293	33.205532089, -117.596249485	33.503658101, -117.596249485	33.205532089, -117.249972307
294	21.4274913960001, -157.778625985	21.4626192360001, -157.722086618	21.4626192360001, -157.722086618

§ 202.1401

28 CFR Ch. I (7-1-25 Edition)

TABLE 1 TO § 202.1401—Continued

Area ID	Latitude/longitude coordinates of geofenced areas	
295	21.38026423, -157.914545183	21.392788317, -157.897882367
296	38.4780113490001, -77.609862936	38.6440896410001, -77.6283059322
297	31.5437915750001, -84.095978531	31.5617240260001, -84.007643854
298	34.434594240001, -116.97121195	34.8453594240001, -116.909128396
299	38.5154624890001,	38.52535364690001,
	-77.37115109999	-77.3589766938999
300	30.391006078, -81.537656096	30.413437169, -81.537656096
301	38.828254514, -77.120041471	38.831963061, -77.120041471
302	39.32514001, -76.4241855929999	39.337202481, -76.4241855929999
303	48.126874690001, -122.17560321	48.1263336970001, -122.168283314
304	32.365364879, -86.376531674	32.415623844, -86.376531674
305	21.3463896610001, -157.73213131	21.3809869910001, -157.706839578
306	34.75300134, -96.021930066	34.887500702, -96.021930066
307	38.6375594030001, -121.4291885	38.6902393680001, -121.4291885
308	37.5874487980001, -97.29829204	37.6560529890001, -97.29829204
309	33.90292894, -80.822110255	33.94386779, -80.822110255
310	35.800297926, -81.3673843	33.94386779, -80.780803864
311	38.36798888, -81.594851531	33.94386779, -80.780803864
312	32.7348147280001, -117.209483129	32.7455697900001, -117.184267844
313	34.214686409, -103.86383499	34.383336857, -103.668563532
314	35.021000832, -89.9701571149999	35.030015831, -89.9701571149999
315	35.815792568, -88.754238681	35.9461603686, -88.646037805
316	38.015441735, -122.065438909	38.015441735, -121.969625159
317	33.95602930001,	33.94386779, -80.780803864
	-78.0749560269999	-78.0749560269999
318	44.883655020001, -93.222511412	44.883655020001, -93.19773597
319	48.3955222490001, -101.391958779	48.4441800980001, -101.29867086
320	32.792070847, -117.105638208	32.815052529, -117.08133666
321	32.02879454, -86.41067215	32.030654183, -86.346469999
322	30.935302703, -83.212006939	31.0144779318, -83.212006939
323	43.0246506180001, -115.886565384	43.0755981900001, -115.836215987
324	39.44196171, -85.545889497	39.059128926, -85.545889497
325	32.8074254520001, -115.688918811	32.8401116740001, -115.646437997
326	28.5876565020001, -97.628083873	28.6265342520001, -97.584908779
327	71.31064894, -156.674424861	71.34423366, -156.617754628
328	43.859737320001, -69.95330606	43.9103207020001, -69.909873769
329	32.745470783, -97.44549275	32.787133199, -97.413267401
330	30.19410042770001,	30.2458023780001,
	-81.7076006299999	-81.1659334233999
331	40.1857296150001, -75.164926593	40.2167846540001, -75.134209434
332	24.5560939770001, -81.722408305	24.5971158050001, -81.653518462
333	27.467423380001, -97.832157771	27.5231989330001, -97.788047634
334	36.386386503, -119.977147505	36.386386503, -119.869576662

Department of Justice

§ 202.1401

335	30.326507308, -87.352445013	30.375924031, -87.352445013	30.375924031, -87.352445013	30.326507308, -87.257235015.
336	30.888811264, -87.043781272	30.738102029, -87.043781272	30.738102029, -86.997376436	30.6838811264, -86.997376436.
337	36.106368485, -86.671148	36.114637747, -86.6786059	36.114637747, -86.6786059	36.106368485, -86.671148
338	32.6686509240001, -117.14230685	32.6740385570001, -117.114230685	32.6740385570001, -117.114230685	32.6686509240001, -117.114230685
339	38.974689920001,	39.0026084470001,	39.0026084470001,	38.974689920001,
340	-76.4937690629999,	27.718208017, -97.4505952709999	27.718208017, -97.4505952709999	-76.448781289999,
341	29.801429860001,	29.8575240390001,	29.8575240390001,	29.801429860001,
342	32.498252175, -88.6318691439999	32.602832677, -88.6318691439999	32.602832677, -88.6318691439999	32.498252175, -88.5064742839999,
343	36.7852781730001, -76.06232016	36.8386906080001, -76.06232016	36.8386906080001, -76.06232016	36.7852781730001, -75.9981255
344	36.76031462, -75.9846076869999	36.81818534, -75.940981369999	36.81818534, -75.940981369999	36.76031462, -75.940981369999
345	38.2488191400001, -76.46369128	38.3093935480001, -76.46369128	38.3093935480001, -76.46369128	38.2488191400001, -76.373549279,
346	48.311418739, -122.70896597	48.36970655, -122.70896597	48.36970655, -122.617753395	48.311418739, -122.617753395
347	55.2654343400001, -117.1890231	56.2318077000001, -117.1890231	56.2318077000001, -117.1890231	55.2654343400001, -116.9249447,
348	13.30510949700001, -144.618332428	13.588322610001, -144.618332428	13.588322610001, -144.618332428	13.30510949700001, -144.618357575
349	47.6909210600001, -122.628044406	47.705184112, -122.628044406	47.705184112, -122.628044406	47.6909210600001, -122.613798201,
350	47.677991730001, -122.74742327	47.7726169310001, -122.74742327	47.7726169310001, -122.74742327	47.677991730001, -122.691789797,
351	47.54493861660001, -122.671768178	47.55653870590001, -122.671768178	47.55653870590001, -122.671768178	47.54493861660001, -122.623883723,
352	32.675119312, -117.256218377	32.713082807, -117.256218377	32.713082807, -117.256218377	32.675119312, -117.234025189,
353	32.6629355910001, -117.159777498	32.6684545140001, -117.159777498	32.6684545140001, -117.159777498	32.6629355910001, -117.12975083,
354	34.0808098932, -119.160456826	34.13946678, -119.160456826	34.13946678, -119.160456826	34.0808098932, -119.064148436,
355	34.14295682, -119.221480878	34.175763756, -119.221480878	34.175763756, -119.221480878	34.14295682, -119.195140105,
356	55.5394977110001, -131.764707731	55.54297949870001, -131.764707731	55.54297949870001, -131.764707731	55.5394977110001, -131.755720856,
357	46.3564572000001,	46.37438300209999	46.37438300209999	46.3564572000001,
358	-98.3483200209999	-98.3483200209999	-98.3483200209999	-98.3483200209999
359	28.581333934, -67.18385157	28.586385157, -67.18385157	28.586385157, -67.18385157	28.586385157, -67.18385157
360	18.3928272859, -67.183834374	18.405878229, -67.183834374	18.405878229, -67.183834374	18.405878229, -67.183834374
361	44.6222594310001, -67.32822059	44.7036300010001, -67.32822059	44.7036300010001, -67.32822059	44.6222594310001, -67.32822059
362	38.8918607040001, -77.070549603	38.924172190001, -77.070549603	38.924172190001, -77.070549603	38.8918607040001, -77.063519892,
363	38.820046750001, -77.027450812	38.8300442400001, -77.027450812	38.8300442400001, -77.027450812	38.820046750001, -77.017462058,
364	38.406152209, -77.1013740786	38.417284684, -77.1013740786	38.417284684, -77.1013740786	38.406152209, -77.072946836999,
365	30.33369265, -89.6481721	30.417826484, -89.6481721	30.417826484, -89.6481721	30.33369265, -89.557854425,
366	38.679074200001, -76.3415482	38.6792870940001, -76.3415482	38.6792870940001, -76.3415482	38.679074200001, -76.343227801,
367	42.3047750280001, -76.34950294	42.3249165250001, -76.34950294	42.3249165250001, -76.34950294	42.3047750280001, -76.34950294
368	41.503225932, -71.30984392	41.554068671, -71.30984392	41.554068671, -71.30984392	41.503225932, -71.30984392
369	36.9170290100001, -76.335615748	36.9404015810001, -76.335615748	36.9404015810001, -76.335615748	36.9170290100001, -76.335615748
370	30.748875362, -81.576797991	30.837030033, -81.576797991	30.837030033, -81.576797991	30.748875362, -81.47993971,
371	41.3859706700001, -72.0385059	41.4104621860001, -72.0385059	41.4104621860001, -72.0385059	41.3859706700001, -72.07728596,
372	36.8809746340001, -76.42731462	36.880977200001, -76.42731462	36.880977200001, -76.42731462	36.8809746340001, -76.419013745,
373	38.7449505, -86.905209651	38.919755552, -86.905209651	38.919755552, -86.905209651	38.7449505, -86.678811986999,
374	30.152883738, -85.760741626	30.188382598, -85.760741626	30.188382598, -85.760741626	30.188383738, -85.73893885,
375	40.0361710100001, -75.101397768	40.0471374300001, -75.101397768	40.0471374300001, -75.088731354,	40.0361710100001, -75.088731354,
376	38.871250644, -76.99841861999	38.976565839, -76.99841861999	38.976565839, -76.99841861999	38.871250644, -76.991241863999,
377	38.3186054830001, -77.051455995	38.3591595940001, -77.051455995	38.3591595940001, -77.051455995	38.3186054830001, -77.014266139,
378	38.5619658580001, -77.210364797999	38.6060805630001, -77.210364797999	38.6060805630001, -77.210364797999	38.5619658580001, -77.014266139,
379	47.9738990070001, -116.566365931	47.9810063290001, -116.566365931	47.9810063290001, -116.566365931	47.9738990070001, -116.520622995,

§ 202.1401

28 CFR Ch. I (7-1-25 Edition)

TABLE 1 TO § 202.1401—Continued

Area ID		Latitude/longitude coordinates of geofenced areas
380	40.2823128210001, -74.214186736	40.2823128210001, -74.214186736
381	33.9177546080001, -117.576534598	33.931444460001, -117.562312486
382	37.208022726, -76.633932842	37.273612882, -76.633932842
383	45.322559620001, -119.895359741	45.806555030001, -119.455477367
384	32.681825013, -117.22971083	32.715125046, -117.22971083
385	36.842303428, -76.151234269999	36.842303428, -76.151234269999
386	35.180388117, -111.749899999	35.195319693, -111.736545714
387	40.6710820530001, -112.091693872	40.6820119650001, -112.091693872
388	37.4104380160001, -122.0315458936	37.4153630160001, -122.0315458936
389	47.966605751, -122.271045712	47.994496312, -122.271045712
390	30.361267243, -81.4636657189999	30.400329774, -81.4636657189999
391	38.976796961, -76.4937690629999	38.986732986, -76.4937690629999
392	38.9970659050001, -77.097142558	39.0074154440001, -77.097142558
393	36.9181778190001, -76.317281615	36.933520845, -76.317281615
394	40.216016376, -77.001594842	40.239975455, -77.001594842
395	35.3183642820001, -89.890382347	35.3408744740001, -89.890382347
396	36.595508146, -121.878756787	36.60645199, -121.878756787
397	36.8096651020001, -76.311406446	36.82836800001, -76.311406446
398	32.384281564, -80.685725766	32.394141164, -80.685725766
399	33.726669684, -118.099622184	33.774096004, -118.099622184
400	36.58722707780001, -121.86360531	36.5945029280001, -121.86360531
401	36.203462880001, -115.073249953	36.399515790001, -115.073249953
402	36.466851030001, -117.08418948	37.0076912670001, -117.08418948
403	42.919235051, -71.671337464	42.952654138, -71.671337464
404	39.6829375310001, -75.600492457	39.6923952360001, -75.600492457
405	43.107473267, -70.787901469	43.107471, -70.787901469
406	33.565982911, -86.751872966	33.57308195, -86.751872966
407	61.598428526, -149.39005833	61.606721914, -149.39005833
408	36.013579803, -115.202476534	36.020786485, -115.202476534
409	45.1080754539, -93.178546539	45.1080754539, -93.178546539
410	33.7189514350001, -84.361650185	33.7254539750001, -84.361650185
411	44.08085533, -70.290540358	44.094617619, -70.290540358
412	42.542571763, -71.589424731	42.551133712, -71.589424731
413	44.8040301450001, -88.9467649249999	44.8172629220001, -88.9467649249999
414	30.354065667, -91.146045237	30.360422127, -91.146045237
415	31.4025019330001, -92.335343385	31.479576740001, -92.335343385
416	40.087768460001, -83.068853255	40.0907737950001, -83.068853255
417	44.022196352, -121.133291563	44.028392756, -121.133291563
418	30.173439579, -97.674627878	30.17858121, -97.674627878
419	38.54450506760001, -75.068273519999	38.551078790001, -75.068273519999
420	44.101651610001, -121.17360693	44.3272733540001, -121.058161787

421	46.827120683, -100.725445186	46.832772324, -100.725445186	46.832772324, -100.715045706	46.827120683, -100.715045706
422	44.392304805, -70.94712474	44.402273905, -70.94712474	44.402273905, -70.928234819	44.392304805, -70.928234819
423	47.549068751, -122.684072241	47.556350796, -122.684072241	47.556350796, -122.678571789	47.549068751, -122.678571789
424	33.4426391850001, -112.60336981	33.4938449270001, -112.60836981	33.4938449270001, -112.590831261	33.4426391850001, -112.590831261
425	41.78965498, -90.0518139389999	41.78965498, -90.0518139389999	41.78965498, -90.0425795319999	41.78965498, -90.0425795319999
426	44.70559069, -123.251143191	44.70559069, -123.251143191	44.70559069, -123.251143191	44.70559069, -123.251143191
427	41.906850084, -96.34425821	41.906850084, -96.34425821	41.906850084, -96.326681639	41.906850084, -96.326681639
428	39.2163293430001, -86.978574079999	39.39294468560001, -86.978574079999	39.39294468560001, -86.978574079999	39.2163293430001, -86.978574079999
429	31.36616242780001, -92.4083963209999	31.3916242780001, -92.4083963209999	31.3916242780001, -92.3606840609999	31.36616242780001, -92.3606840609999
430	31.646126890001, -98.960277256	31.666772080001, -98.960277256	31.666772080001, -98.960277256	31.646126890001, -98.960277256
431	41.607733723, -71.505549174	41.623638419, -71.505549174	41.623638419, -71.491180453	41.607733723, -71.491180453
432	47.6525289910001, -98.9417110537999	48.063600830001, -98.9417110537999	48.063600830001, -98.86003788309999	47.6525289910001, -98.86003788309999
433	35.5952678190001, -95.22118754	35.7838291280001, -95.22118754	35.7838291280001, -95.126697455	35.5952678190001, -95.126697455
434	41.939462950001, -72.670901858	41.9441994120001, -72.670901858	41.9441994120001, -72.661211157	41.939462950001, -72.661211157
435	34.812473220001, -92.3897548209999	34.961487718001, -92.3897548209999	34.961487718001, -92.3897548209999	34.812473220001, -92.3897548209999
436	30.3094558060001, -97.78694553	30.3273409100001, -97.78694553	30.3273409100001, -97.756391927	30.3094558060001, -97.756391927
437	33.774194279, -95.606477742	33.882753059, -95.606477742	33.882753059, -95.526066392	33.774194279, -95.526066392
438	32.5353248810001, -93.475517374	32.5878534930001, -93.475517374	32.5878534930001, -93.320012082	32.5353248810001, -93.320012082
439	41.3242015147, -72.192567648	41.334274179, -72.192567648	41.334274179, -72.1830023	41.3242015147, -72.1830023
440	43.287221800001, -116.0973157	43.604674600001, -116.0973157	43.604674600001, -116.00627152	43.287221800001, -116.00627152
441	41.5256110640001, -83.029247488	41.5564763520001, -83.029247488	41.5564763520001, -83.011533492	41.5256110640001, -83.011533492
442	44.0771040870001, -103.272190023	44.0820854380001, -103.272190023	44.0820854380001, -103.262202287	44.0771040870001, -103.262202287
443	41.12310363250001, -81.1929117339999	41.2310363250001, -81.1929117339999	41.2310363250001, -80.97584481	41.12310363250001, -80.97584481
444	-81.1929117339999	-81.1929117339999	-81.1929117339999	-81.1929117339999
445	46.07228877, -94.556923336	46.331943757, -94.556923336	46.331943757, -94.325692646	46.07228877, -94.325692646
446	39.34639557, -82.9650961519999	39.360752962, -82.9650961519999	39.360752962, -82.93837729999	39.34639557, -82.93837729999
447	41.29766303, -73.975066263	41.342571403, -73.975066263	41.342571403, -73.930650098	41.29766303, -73.930650098
448	30.213250780001, -97.33768878	30.319193057, -97.33768878	30.319193057, -97.247469425	30.213250780001, -97.247469425
449	43.922486604, -90.27680935	43.982150434, -90.27680935	43.982150434, -90.261339487	43.922486604, -90.261339487
450	45.4105970370001, -122.564234834	45.414613790001, -122.546020519	45.414613790001, -122.546020519	45.4105970370001, -122.546020519
451	30.19297926, -91.13649361	30.20995846, -91.13649361	30.20995846, -91.120742129	30.19297926, -91.120742129
452	33.671676665, -86.017370951	33.757794604, -86.017370951	33.757794604, -85.38821888551	33.671676665, -85.38821888551
453	40.2117159210001, -75.432393416	40.2164501770001, -75.432393416	40.2164501770001, -75.42374491	40.2117159210001, -75.42374491
454	33.6765084310001, -88.7534024129999	-89.7534024129999	-89.6202355929999	33.6765084310001, -89.6202355929999
455	39.37852207, -79.708317675	39.454188743, -79.708317675	39.454188743, -79.639802717	39.37852207, -79.639802717
456	42.27527302, -85.3763242809999	42.336654723, -85.3763242809999	42.336654723, -85.276449549999	42.27527302, -85.276449549999
457	34.222785926, -84.114704149999	34.225953578, -84.114704149999	34.225953578, -84.111527931999	34.222785926, -84.111527931999
458	46.8328736340001, -92.159841749999	46.8342828600001,	46.8342828600001,	46.8328736340001,
459	43.14072293, -115.657766227	43.147959584, -115.657766227	43.147959584, -115.647820427	43.14072293, -115.647820427
460	38.949813614, -79.985745343	38.958420468, -79.985745343	38.958420468, -79.972014372	38.949813614, -79.972014372
461	31.3824479320001, -92.31791139	31.4098514070001, -92.31791139	31.4098514070001, -92.279692875	31.3824479320001, -92.279692875
462	44.498956200001, -73.14626073	44.5216654230001, -73.14626073	44.5216654230001, -73.151341101	44.498956200001, -73.151341101
463	33.05649478, -111.387806148	33.118281303, -111.387806148	33.118281303, -111.387806148	33.05649478, -111.318954206

§ 202.1401

28 CFR Ch. I (7-1-25 Edition)

TABLE 1 TO § 202.1401—Continued

Area ID	Latitude/longitude coordinates of geofenced areas	
464	36.276929619, -115.061711815	36.307014017, -115.024997297
465	36.9652916110001, -78.019676053	37.1220791840001, -77.838575255
466	35.177556188, -94.342568303	35.36254474, -94.342568303
467	40.3805917540001, -76.70923494	40.4828843550001, -76.526125382
468	33.72733962760001, -85.799971241	33.7412047100001, -85.777787227
469	32.83483698330001,	32.83483698330001,
	-98.0657312119999,	-97.9964332399999,
470	32.775847904, -97.4626718379999	32.781682325, -97.4626718379999
471	38.1716157600001, -84.921446944	38.1966286800001, -84.921446944
472	18.002735849, -66.5139236319999	18.025884249, -66.5139236319999
473	21.257388270001, -157.811868495	21.2696069800001, -157.811868495
474	33.910428789, -84.5367196229	33.910428789, -84.522565546
475	40.959663633, -98.301445179	40.964149849, -98.296290336
476	40.515397589, -98.298239402	40.567785704, -98.259993615
477	13.471680227, -144.807392696	13.476444623, -144.812849999
478	30.40405289490001, -89.05284316	30.4205257120001, -89.059168989
479	30.520223183, -90.417497467	30.526889408, -90.417497467
480	39.528072455, -76.1100913129999	39.528072455, -76.1100913129999
481	46.6059564510001, -111.975646726	46.6106942060001, -111.975646726
482	40.4376721520001,	40.4407479890001,
	-78.4170869399999,	-78.4170869399999,
483	43.658487912, -70.674868746	43.679892728, -70.654823081
484	39.7424976190001, -86.220956444	39.7462615480001, -86.225390797
485	35.3048305880001, -72.778800001	35.3717978800001, -72.664040578
486	35.594877558, -88.91639526	35.601416549, -88.91639526
487	29.9497813040001,	29.9740232620001,
	-90.0120171797999,	-89.99878208999,
488	38.8833909860001,	38.905765642, -81.8464496549999
	-81.8464496549999,	-81.8464496549999
489	39.0160591, -95.6872730109999	39.022374526, -95.6872730109999
490	36.4178126140001, -82.493381518	36.4246402130001, -82.493381518
491	21.31427856330001, -158.069986235	21.3240454770001, -158.069986235
492	39.76427925, -65.52719456	39.778947386, -65.508366982
493	44.0647301730001, -122.982252253	44.0670417360001, -122.973786312
494	42.766339845, -84.576207556	42.763800145, -84.567413358
495	32.270748628, -106.939139534	32.28928019, -106.939139534
496	40.2658142880001, -74.748095306	40.273412650001, -74.740257715
497	35.0150424290001, -97.23911654	35.0295356340001, -97.223711786
498	40.835606820001, -96.758767006	40.8404020610001, -96.749174181
499	33.7812312280001, -118.067627933	33.8016134000001, -118.032767969
500	32.8597198360001,	32.8630748340001,
	-83.6073436619999,	-83.6073436619999
501	39.636663701, -92.534704178	39.721017576, -92.534704178
502	41.305913573, -88.7046910729999	41.305913573, -88.6608137729999

Department of Justice

§ 202.1401

503	29.429494618, -98.3843199139999	29.437625079, -98.3746227379999	29.426494618, -98.3746227379999
504	39.7487626001, -81.84706613	39.7487626001, -81.84706613	39.7487626001, -81.84706613
505	44.9048285740001, -123.03047071	44.9170262920001, -123.03047071	44.9170262920001, -123.03047071
506	41.1829896970001, -96.49160163	41.2049128990001, -96.49160163	41.2049128990001, -96.49160163
507	37.6700185530001, -98.267361175	37.6583757600001, -98.267361175	37.6583757600001, -98.267361175
508	32.40318517050001, -86.247361114	32.4082452810001, -86.247361114	32.4082452810001, -86.247361114
509	36.1649285010001, -78.8353628877	36.2232305700001, -78.8353628877	36.2232305700001, -78.8353628877
510	37.8823890080001, -94.38772354	37.8823890080001, -94.38772354	37.8823890080001, -94.38772354
511	36.757597445450001, -94.38772354	36.8328900800001, -94.38772354	36.8328900800001, -94.38772354
512	42.526779020001, -71.06205514	42.5603767370001, -71.06205514	42.5603767370001, -71.06205514
513	39.47196387830001, -76.8607346809999	39.5047196387830001, -76.8607346809999	39.5047196387830001, -76.8607346809999
514	46.1080148720001, -123.964495138	46.1501140200001, -123.964495138	46.1501140200001, -123.964495138
515	17.9872857480001, -66.333706182	18.0655436220001, -66.333706182	18.0655436220001, -66.333706182
516	33.78725571163, -82.2952040439999	33.807394959, -82.2952040439999	33.807394959, -82.2952040439999
517	46.6005921770001, -112.190250013	46.6592451280001, -112.190250013	46.6592451280001, -112.190250013
518	39.224556381, -76.1081268	39.337394743, -76.1081268	39.337394743, -76.1081268
519	46.220501032, -111.635118944	46.337394743, -111.635118944	46.337394743, -111.635118944
520	42.1437134500001, -104.948278887	42.4788211760001, -104.948278887	42.4788211760001, -104.948278887
521	35.65608251539, -95.375341077	35.6648813430001, -95.375341077	35.6648813430001, -95.375341077
522	36.1023248190001, -86.715681439999	36.1023248190001, -86.715681439999	36.1023248190001, -86.715681439999
523	40.9786718780001, -80.325759923	40.9800945050001, -80.325759923	40.9800945050001, -80.325759923
524	35.2623862810001, -97.4851407689999	35.2681205600001, -97.4851407689999	35.2681205600001, -97.4851407689999
525	33.61517453390001, -84.3128273029999	33.6193347170001, -84.3128273029999	33.6193347170001, -84.3128273029999
526	33.4618850200001, -111.969623276	33.472756758900001, -111.969623276	33.472756758900001, -111.969623276
527	32.657784646960001, -111.495190228	32.6688813430001, -111.495190228	32.6688813430001, -111.495190228
528	35.904715505, -78.715406802	35.918095505, -78.715406802	35.918095505, -78.715406802
529	39.8002476900001, -82.9570252779999	39.809855625370001, -82.9570252779999	39.809855625370001, -82.9570252779999
530	35.3777455200001, -106.65493619	35.39773832105, -75.6147487649999	35.39773832105, -75.6147487649999
531	39.66393073710001, -92.433535397	43.9977499120001, -92.433535397	43.9977499120001, -92.433535397
532	43.9963073710001, -92.433535397	44.7488170001, -93.1288170001	44.7488170001, -93.1288170001
533	47.7438511480001, -86.3980685539999	32.295043619, -86.3980685539999	32.295043619, -86.3980685539999
534	32.8247954014, -97.3530695539999	32.861579522, -97.3530695539999	32.861579522, -97.3530695539999
535	37.03064888, -113.549169301	37.03178732, -113.549169301	37.03178732, -113.549169301
536	37.887174903900001, -97.642976177	37.887174903900001, -97.642976177	37.887174903900001, -97.642976177
537	37.49085725, -77.311608389999	37.498350787, -77.311608389999	37.498350787, -77.311608389999
538	35.6282856160001, -106.764286388	35.5517461870001, -106.764286388	35.5517461870001, -106.764286388
539	40.117249027480001, -74.044914025	40.12989027480001, -74.044914025	40.12989027480001, -74.044914025
540	39.580378098, -85.816200007	39.580378098, -85.816200007	39.580378098, -85.816200007
541	32.517987523, -111.340100133	32.5257987523, -111.340100133	32.5257987523, -111.340100133
542	43.5730620240001, -86.67598762029999	43.5883048400001, -86.67598762029999	43.5883048400001, -86.67598762029999
543	-96.6930749859999	-96.6930749859999	-96.6930749859999
544	25.961807289730001, -80.31070355	25.961807289730001, -80.31070355	25.961807289730001, -80.31070355
545	38.1950135365, -89.745598204	38.1950135365, -89.745598204	38.1950135365, -89.745598204
546	40.188081510001, -75.561069736	40.188081510001, -75.561069736	40.188081510001, -75.561069736

§ 202.1401

28 CFR Ch. I (7-1-25 Edition)

TABLE 1 TO § 202.1401—Continued

Area ID	Latitude/longitude coordinates of geofenced areas	
547	39.816093520001, -89.673473292	39.83006927080001, -89.673473292
548	37.248049060001, -93.395772062	37.2571610570001, -93.395772062
549	45.532774400001, -94.060606066	45.5419761270001, -94.060606066
550	45.564507200001, -94.179496597	45.565242030001, -94.179496597
551	36.8110053880001,	36.8227443260001,
552	-75.9894743689989	-75.9894743689989
553	41.3451753470001, -72.293373883	41.3815369730001, -72.293373883
554	36.285684226, -95.309758124	36.300130892, -95.309758124
555	43.2708696780001,	-71.128820539999,
556	44.49653945450001, -73.168838485	44.5034995450001, -73.168838485
557	44.442952367, -72.960320316	44.500157333, -72.960320316
558	38.546453582, -92.080098162	38.556080633, -92.080098162
559	19.696784088, -155.052848025	19.715068265, -155.052848025
560	36.8786769800001, -90.310798339	36.9046015270001, -90.310798339
561	34.9067538820001, -85.070727678	34.9506642170001, -85.070727678
562	35.814732012, -72.9234741183999	35.820152012, -72.9234741183999
563	36.006276454, -86.516501852	36.027518046, -86.516501852
564	44.067527784, -103.325214534	44.0784787400001, -103.325214534
565	43.0853898060001,	-78.9722862539999,
566	37.2459669890001, -87.264708666	37.3155568590001, -87.264708666
567	39.348643610001, -81.448406511	39.348643610001, -81.448406511
568	43.230983715, -78.987693814	43.244098627, -78.987693814
569	38.414110285, -90.4008815851999	38.519393631, -90.4008815851999
570	43.1058774480001,	-78.9722862539999,
571	38.8465829040001,	38.8511023340001,
572	-72.4562338169999,	-72.4562338169999,
573	36.798812242, -76.292826352	36.806581273, -76.291663588
574	36.824516203, -76.291110961999	36.82654125, -76.291110961999
575	31.03987980001, -77.07676692	31.03987980001, -77.07676692
576	30.48569113, -86.966749359	30.523283452, -86.966749359
577	31.403383560001, -87.057347927	31.4251772980001, -87.057347927
578	30.41755556, -86.90261039999	30.423862018, -86.90261039999
579	30.595791442, -86.950876547	30.619098213, -86.950876547
580	30.617963515, -87.148395847	30.632703528, -87.148395847
581	30.49807584, -87.662644784999	30.520323757, -87.662644784999
582	30.33836652, -87.54959867999	30.35197261, -87.54959867999
583	35.381397860001, -89.875828209	35.3503400000001, -89.875828209
584	36.5535830635, -76.292027831	36.5580439287, -76.292027831

585	33.891359251, -118.072946629	33.894991619, -118.067394654	33.891359251, -118.067394654
586	38.324233070001, -76.4841629759999	38.344233070001, -76.4841629759999	38.324233070001, -76.4841629759999
587	43.077684909, -73.823802707	43.082196882, -73.823802707	43.077684909, -73.818216923
588	18.4276186450001, -66.188700669	18.4276186450001, -66.188700669	18.4276186450001, -66.188700669
589	35.086256399, -90.1438097929999	35.090263498, -90.1438097929999	35.086256399, -90.1438097929999
590	42.4740966470001, -71.292022302	42.4801271500001, -71.292022302	42.4740966470001, -71.292022302
591	41.098262130001, -95.9280611469999	41.1364452900001, -95.9280611469999	41.098262130001, -95.9280611469999
592	32.745230660001, -117.200217282	32.752565660001, -117.200217282	32.752565660001, -117.192605845
593	32.783231948, -88.8528249177999	32.8145254912, -88.8528249177999	32.783231948, -88.8124127399999
594	30.37231968, -87.429057305	30.394059181, -87.429057305	30.37231968, -87.396697185
595	48.1708872200016, -122.648186576	48.2120255960001, -122.648186576	48.1708872200016, -122.615173447
596	30.338350216, -81.889129182	30.377897748, -81.889129182	30.338350216, -81.84492402
597	70.488162834, -149.926235024	70.509905742, -149.926235024	70.488162834, -149.855544128
598	43.098523532, -116.31428757	43.37173967, -116.31428757	43.37173967, -115.957075202
599	38.0284346090001, -122.170412652	38.0284346090001, -122.170412652	38.0284346090001, -122.162692799
600	21.979075729, -159.787865529	22.07350219, -159.787865529	21.979075729, -159.78643749
601	37.705457716, -121.91515472	37.747451286, -121.91515472	37.705457716, -121.871676143
602	28.2124892410001, -80.6189925999999	28.2719774110001, -80.6189925999999	28.2124892410001, -80.5967212699999
603	21.3812710710001, -157.972837384	21.3857579590001, -157.972837384	21.3857579590001, -157.969830103
604	43.0820098340001, -70.8265631579999	43.095680228, -70.8265631579999	43.095680228, -70.8118178159999
605	-70.8265631579999	-70.8265631579999	-70.8265631579999
606	38.805877954, -104.720171001	38.8838836254, -104.720171001	38.805877954, -104.673427575
607	40.9140582660001, -74.590780383	40.9856152640001, -74.590780383	40.9140582660001, -74.49014259
608	18.26752057, -65.759072139	18.26922761, -65.759072139	18.26922761, -65.75902273
609	37.495160689, -122.50068813	37.504556663, -122.50068813	37.495160689, -122.4941686302
610	34.270207210001, -92.1396888	34.3785932240001, -92.1396888	34.270207210001, -92.033468658
611	18.2467234310001, -65.600381523	18.2570859030001, -65.600381523	18.2467234310001, -65.582259288999
612	37.33590329, -104.173059108	37.644554428, -104.173059108	37.33590329, -103.576450075
613	40.489967436, -80.215160815	40.489967436, -80.215160815	40.489967436, -80.20567052
614	40.489953950001, -80.215160811	40.497931050001, -80.215160811	40.489953950001, -80.205680084
615	19.58002141, -155.753584385	19.985340889, -155.753584385	19.935340889, -155.482149063
616	33.737688318, -80.516830485999	33.849728431, -80.516830485999	33.849728431, -80.445008049999
617	38.887515787, -123.552272552	38.895551718, -123.552272552	38.895551718, -123.538718114
618	71.32665191, -156.649567453	71.336534761, -156.649567453	71.336534761, -156.601540334
619	45.57436111, -122.60483246	45.583315392, -122.60483246	45.583315392, -122.585382407
620	42.908782210001, -43.987032990001	42.908782210001, -43.987032990001	42.908782210001, -43.987032990001
621	-71.4221747879999	-71.4221747879999	-70.722436956
622	36.594597106, -121.926941695	36.608467628, -121.926941695	36.594597106, -121.894607972
623	38.263920139, -104.386287178	38.360999196, -104.386297178	38.263920139, -104.275724057
624	38.29060253, -77.067130082999	38.31683736, -77.067130082999	38.29060253, -77.017063118999
625	21.3139823400001, -157.982793478	21.3226045200001, -157.982793478	21.3139823400001, -157.982066252
626	41.5907533400001, -71.4234866	41.6007626130001, -71.418791	41.5907533400001, -71.418791
627	37.163382287, -80.579118870999	37.207412609, -80.51012826999	37.163382287, -80.51012826999
627	18.5087916470001, -67.098861576	18.5101598370001, -67.098861576	18.5087916470001, -67.0988621282

§ 202.1401

28 CFR Ch. I (7-1-25 Edition)

TABLE 1 TO § 202.1401—Continued

Area ID	Latitude/longitude coordinates of geofenced areas	
628	33.397278645, -94.4116858869999	33.464838472, -94.3047919909999
629	44.9551877580001, -70.513638005	45.0169721250001, -70.513638005
630	34.550284843, -86.723778349999	34.710910354, -86.723778349999
631	39.4978523080001, -119.778804811	39.5025454730001, -119.778804811
632	39.806889794, -82.949783742	39.819444008, -82.949783742
633	38.1508457900001, -78.41805901	38.1586875900001, -78.41805901
634	37.7110124880001, -120.921809782	37.7227924600001, -120.921809782
635	32.5734846130001, -83.613041736	32.6644753900001, -83.613041736
636	41.5101975790001, -90.566624136	41.5236820390001, -90.566624136
637	39.816797712, -104.880637268	39.895272909, -104.880637268
638	61.75264087, -166.062507434	61.799913075, -166.062507434
639	39.2183363890001, -75.415282906	39.769793541, -94.904952104
640	39.762626991, -94.904952104	39.897835881, -94.904952104
641	31.342942350001,	31.3453725330001, -86.08558079
	-86.0977289259999	-86.0977289259999
642	40.7858318330001, -111.959489583	40.7949147800001, -111.953251907
643	32.8003673640001, -118.606292107	33.0377362220001, -118.606292107
644	33.29562044, -119.582134532	34.062044, -118.348994062
645	33.7662733170001, -118.309265541	33.7813000720001, -118.309265541
646	33.991029047, -119.635878529	33.99744378, -119.635878529
647	30.456179089, -87.351595059	30.456179089, -87.351595059
648	42.1757726720001,	42.284196191, -90.4077834729999
	-90.4077834729999	-90.4077834729999
649	32.119801635, -81.1976234959999	32.13505162, -81.1976234959999
650	42.592501000001, -115.678838723	42.8511848830001, -115.678838723
651	42.843685100001, -73.982567765	42.8583933770001, -73.982567765
652	38.784350810001, -104.551986183	38.801042480001, -104.551986183
653	38.585372905, -89.882877352	38.585372905, -89.882877352
654	41.402655098, -75.667910109999	41.405858099, -75.6679100109999
655	36.9172616480001, -76.32086974	36.9234759510001, -76.31089014
656	48.26740571, -122.645903557	48.3084303770001, -122.645903557
657	42.594400000001,	42.6303400000001,
	-82.8511999999999	-82.8511999999999
658	36.237894413, -119.894821285	36.250497998, -119.8869682611
659	60.131877020001, -149.434449035	60.1347511870001, -149.434449035
660	35.321463870001, -77.99707351	35.368940398, -77.99707351
661	33.9505024190001, -80.494323712	33.9954038330001, -80.494323712
662	31.3562318730001, -85.85688056	31.3677829840001, -85.85688056
663	33.956330827, -98.528137562	34.017271784, -98.528137562
664	40.1402214600001, -120.185906595	40.2702161240001, -120.185906595
665	32.585610327, -117.134530157	32.609517949, -117.134530157
666	42.3865801530001, -96.37733927	42.399885140001, -96.37733927
667	31.2921867390001, -86.135253897	31.2921867390001, -86.135253897
	-96.3700527519999	-96.3700527519999
	31.2921867390001, -86.12630462	31.2921867390001, -86.12630462

Department of Justice

§ 202.1401

668	38.5971126590001, -97.881769008	38.7549420740001, -97.891769008	38.5971126590001, -97.731700038
669	32.665275626, -117.245056924	32.670651139, -117.245056924	32.665275626, -117.237168813
670	61.118439774, -155.58809541	61.118439774, -155.58809541	61.118439774, -155.58809541
671	39.84525313250001, -83.84415692	39.8525313250001, -83.84415692	39.84525310260001, -83.827046603
672	36.7792288150001, -76.316870104	36.7960357240001, -76.316870104	36.7792288150001, -76.304641406
673	38.5886024650001, -90.211334345	38.5936098780001, -74.096301663	38.5886024650001, -90.205345975
674	41.491597375, -74.096301663	41.493603532, -74.092315153	41.491597375, -74.092315153
675	41.4957478890001, -74.093456875	41.5071142860001, -74.07670535	41.4957478890001, -74.07670535
676	31.3536919110001, -86.019020089	31.3632865050001, -86.009368893	31.3536919110001, -86.009368893
677	38.5366165880001, -77.2462204349998	38.5562248710001, -77.196832760999	38.5366165880001, -77.196832760999
678	43.093425804, -76.13209217	43.105369507, -76.117106326	43.093425804, -76.117106326
679	31.1194652620001, -85.983038227	31.1263987840001, -85.975150114	31.1194652620001, -85.975130114
680	32.90171336, -115.830667748	33.001155638, -115.830667748	32.90171336, -115.679781585
681	62.8648431, -156.051764779	62.942582989, -156.051764779	62.8648431, -156.6649688137
682	32.418304849, -113.683744005	32.912746437, -113.683744005	32.418304849, -112.306115231
683	38.9884924360001, -105.010991219	39.0140804660001, -104.991244919	38.9884924360001, -104.991244919
684	65.55280176001, -168.013053723	65.5830229910001, -168.013053723	65.55280176001, -167.912289962
685	35.384500001, -97.4236989999999	35.4497, -97.4236989999999	35.384500001, -97.352865429999
686	41.1825530900001, -75.443820828	41.2131432310001, -75.443820828	41.1825530900001, -75.411887882
687	41.58166204, -83.794956627	41.593889898, -83.794956627	41.58166204, -83.794956627
688	40.260727630001, -112.49273742	40.5755204400001, -112.49273742	40.260727630001, -112.27908302
689	31.2225159510001, -85.5643695170001	31.2323695170001, -85.5643695170001	31.2225159510001, -85.563616915
690	31.3793557900001, -91.894810498	31.665420230001, -91.894810498	31.3793557900001, -91.52596887
691	38.231289094, -121.98348892	38.284736015, -121.98348892	38.231289094, -121.881230384
692	38.3222869080001, -81.983486122	38.3283652900001, -81.983486122	38.3222869080001, -81.915378048
693	21.351128573, -157.889178476	21.3678121054, -157.889178476	21.351128573, -157.879404163
694	21.464248020001, -152.148379892	21.5218182430001, -158.148373992	21.464248020001, -157.901772211
695	43.1244504040001, -89.341359911	43.1368306370001, -89.341359911	43.1244504040001, -89.328466326
696	24.543363810001, -81.816550797	24.5555228860001, -81.797521593	24.543363810001, -81.797521593
697	24.5614307340001, -81.798222455	24.5672092190001, -81.798222455	24.5614307340001, -81.78264081
698	32.127406367, -110.98507243	32.133967336, -110.98507243	32.127406367, -110.945092818
699	36.2121647440001, -95.878742446	36.2203832320001, -95.878742446	36.2203832320001, -95.888996625
700	45.0719044, -93.181911062	45.104247148, -93.181911062	45.0719044, -93.166136866
701	29.953597589, -85.6870879419999	30.141495697, -85.6870879419999	29.953597589, -85.444998661
702	38.98367955, -76.501046507999	38.992477092, -76.501046507999	38.98367955, -76.486822629999
703	21.469739594, -158.057058607	21.479496623, -158.057058607	21.469739594, -158.05204602
704	38.75030283, -104.304283339	38.795708158, -104.304283339	38.75030283, -104.298582551
705	38.954507850001, -104.910763947	39.0421097770001, -104.910763947	38.954507850001, -104.83083276
706	33.2114718620001, -117.39895734	33.2146081990001, -117.39895734	33.2114718620001, -117.398706525
707	40.339363635, -114.1323986	41.187663286, -114.1323986	40.339363635, -112.775026182
708	36.3075026320001, -97.9326562751	36.364534930001, -97.9326562751	36.3075026320001, -97.899061956
709	34.510789440001, -120.6165844615	34.906980380001, -120.645844615	34.510789440001, -120.43765984
710	43.125429819, -75.5932489149999	43.128384246, -75.5932489149999	43.125429819, -75.5892130629999
711	18.093746783, -65.517122090999	18.0939220238, -65.5171222009999	18.093746783, -65.5081834699999
712	43.919868860001, -90.281512146	44.2491740180001, -90.281512146	43.919868860001, -89.996184063999
713	42.308048614, -85.261730616	42.319058737, -85.261730616	42.308048614, -85.241088866
714	-87.9811739899999	-87.9811739899999	-87.9811739899999

TABLE 1 TO § 202.1401—Continued

Area ID	Latitude/longitude coordinates of geofenced areas	
7715	21.444194852, -158.193880164	21.449106118, -158.193880164
7716	33.428286848, -116.729204555	21.449106118, -158.188834873
7717	40.416716462, -74.0474863319	21.449106118, -158.188834873
7718	42.7515762833, -73.715197659	21.449106118, -158.188834873
7719	38.15160599, -76.4415151439999	21.449106118, -158.188834873
7720	29.948494910001, -90.0376652149999	21.449106118, -158.188834873
7721	40.91742229, -113.701870173	21.449106118, -158.188834873
7722	41.3764009720001, -74.104566558	21.449106118, -158.188834873
7723	42.1732117120001, -72.560346443	21.449106118, -158.188834873
7724	21.48202730001, -158.05113405	21.449106118, -158.188834873
7725	47.6966152880001, -117.582780473	21.449106118, -158.188834873
7726	32.356631690001, -106.751912813	21.449106118, -158.188834873
7727	38.7024149040001, -93.530993696	21.449106118, -158.188834873
7728	-93.5961689999999	21.449106118, -158.188834873
7729	35.40348476, -97.615579224	21.449106118, -158.188834873
7730	30.5215171080001, -88.985120688	21.449106118, -158.188834873
7731	39.7701138860001, -84.122055244	21.449106118, -158.188834873
7732	28.352524233, -98.748507381	21.449106118, -158.188834873
7733	34.8723464400001, -116.88720812	21.449106118, -158.188834873
7734	41.272057920001, -76.4914782399999	21.449106118, -158.188834873
7735	-80.6956297689999	21.449106118, -158.188834873
7736	64.73106276001, -147.051773314	21.449106118, -158.188834873
7737	33.551544978, -114.588511663	21.449106118, -158.188834873
7738	33.551544978, -114.588511663	21.449106118, -158.188834873
7739	73.6657078799999	21.449106118, -158.188834873
7740	-80.6669307879999	21.449106118, -158.188834873
7741	-80.6669307879999	21.449106118, -158.188834873
7742	64.73106276001, -147.051773314	21.449106118, -158.188834873
7743	33.551544978, -114.588511663	21.449106118, -158.188834873
7744	33.551544978, -114.588511663	21.449106118, -158.188834873
7745	73.6657078799999	21.449106118, -158.188834873
7746	-80.6669307879999	21.449106118, -158.188834873
7747	64.73106276001, -147.051773314	21.449106118, -158.188834873
7748	33.551544978, -114.588511663	21.449106118, -158.188834873
7749	33.551544978, -114.588511663	21.449106118, -158.188834873
7750	73.6657078799999	21.449106118, -158.188834873
7751	-80.6669307879999	21.449106118, -158.188834873
7752	64.73106276001, -147.051773314	21.449106118, -158.188834873
7753	33.551544978, -114.588511663	21.449106118, -158.188834873
7754	33.551544978, -114.588511663	21.449106118, -158.188834873
7755	73.6657078799999	21.449106118, -158.188834873
7756	-80.6669307879999	21.449106118, -158.188834873