DEPARTMENT OF JUSTICE

28 CFR Part 202

[Docket No. NSD 104]

RIN 1124–AA01

Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons

AGENCY: National Security Division, Department of Justice.

ACTION: Proposed rule; request for comments.

SUMMARY: The Department of Justice proposes a rule to implement 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), by prohibiting and restricting certain data transactions with certain countries or persons.

DATES: Written comments on this notice of proposed rulemaking (NPRM) must be received by November 29, 2024.

ADDRESSES: You may send comments, identified by Docket No. NSD 104, by either of the following methods:

- *Federal eRulemaking Portal: https://www.regulations.gov.* Follow the instructions for sending comments.
- *Mail:* U.S. Department of Justice, National Security Division, Foreign Investment Review Section, 175 N Street NE, 12th Floor, Washington, DC 20002.

FOR FURTHER INFORMATION CONTACT: Email (preferred): *NSD.FIRS.datasecurity@usdoj.gov.* Otherwise, please contact: Lee Licata, Deputy Chief for National Security Data Risks, Foreign Investment Review Section, National Security Division, U.S. Department of Justice, 175 N Street NE, Washington, DC 20002; Telephone: 202–514–8648.

SUPPLEMENTARY INFORMATION: In accordance with 5 U.S.C. 553(b)(4), a plain language summary of the proposed rule is available at *www.regulations.gov.*

Public Participation

Instructions: We encourage comments to be submitted via *https://www.regulations.gov.* Please submit comments only, include your name and company name (if any), and cite ''Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons'' in all correspondence. Anyone submitting business confidential information should clearly identify the business confidential portion at the time of submission, file a statement justifying nondisclosure and referring to the specific legal authority claimed, and provide a non-confidential version of the submission. For comments submitted electronically containing business confidential information, the file name of the business confidential version should begin with the characters ''BC.'' Any page containing business confidential information must be clearly marked ''BUSINESS CONFIDENTIAL'' at the top of that page. The corresponding non-confidential version of those comments must be clearly marked ''PUBLIC.'' The file name of the nonconfidential version should begin with the character ''P.'' Any submissions with file names that do not begin with a ''BC'' will be assumed to be public and will be posted without change, including any business or personal information provided, such as names, addresses, email addresses, or telephone numbers.

To facilitate an efficient review of submissions, the Department of Justice encourages but does not require commenters to: (1) submit a short executive summary at the beginning of all comments; (2) provide supporting material, including empirical data, findings, and analysis in reports or studies by established organizations or research institutions; (3) describe the relative benefits and costs of the approach contemplated in this NPRM and any alternative approaches; and (4) refer to the specific proposed subpart or defined term to which each comment is addressed. The Department of Justice welcomes interested parties' submissions of written comments discussing relevant experiences, information, and views. Parties wishing to supplement their written comments with a follow-up meeting may request to do so, and the Department of Justice may accommodate such requests as resources permit.

Table of Contents

I. Executive Summary

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 it may enable access by countries of concern or covered persons to government-related data or Americans' bulk U.S. sensitive personal data; and meets other criteria specified by the Order. On March 5, 2024, the National Security Division of the Department of Justice (''DOJ'' or ''the Department'') issued an Advance Notice of Proposed Rulemaking (''ANPRM'') seeking public comment on various topics related to implementation of the Order.[1]

This Notice of Proposed Rulemaking (''NPRM'') addresses the public comments received on the ANPRM, sets forth a proposed rule to implement the Order, and seeks public comment. The proposed rule identifies classes of prohibited and restricted transactions; identifies countries of concern and classes of covered persons with whom the regulations would prohibit or restrict transactions involving government-related data or bulk U.S. sensitive personal data; establishes a process to issue (including to modify or rescind) licenses authorizing otherwise prohibited or restricted transactions and to issue advisory opinions; and addresses recordkeeping and reporting of transactions to inform investigative, enforcement, and regulatory efforts of the Department of Justice.

[1] 89 FR 15780 (Mar. 5, 2024).

II. Background

On February 28, 2024, the President issued Executive Order 14117 (Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern) (''the Order''), pursuant to his authority under the Constitution and the laws of the United States, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*) (''IEEPA''); the National Emergencies Act (50 U.S.C. 1601 *et seq.*) (''NEA''); and title 3, section 301 of the United States Code. In the Order, the President expanded the scope of 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). The President determined that additional measures are necessary to counter the unusual and extraordinary threat to U.S. national security posed by the continuing efforts of certain countries of concern to access and exploit government-related data or Americans' bulk U.S. sensitive personal data.

The Order directs the Attorney General, pursuant to the President's delegation of his authorities under IEEPA, to issue regulations that prohibit or otherwise restrict United States persons from engaging in certain transactions in which a foreign country of concern or national thereof has an interest. Restricted and prohibited transactions include transactions that involve government-related data or bulk U.S. sensitive personal data, are a member of a class of transactions that the Attorney General has determined poses an unacceptable risk to the national security of the United States because the transactions may enable countries of concern or covered persons to access government-related data or bulk U.S. sensitive personal data, and are not otherwise exempted from the Order or its implementing regulations. The Order directs the Attorney General to issue regulations that identify classes of prohibited and restricted transactions; identify countries of concern and classes of covered persons whose access to government-related data or bulk U.S. sensitive personal data poses the national security risk described in the Order; establish a process to issue (including to modify or rescind) licenses authorizing otherwise prohibited or restricted transactions; further define terms used in the Order; address recordkeeping and reporting of transactions to inform investigative, enforcement, and regulatory efforts of the Department of Justice; and to take whatever additional actions, including promulgating additional regulations, as may be necessary to carry out the purposes of the Order.

The Order and this proposed rule fill an important gap in the United States Government's authorities to address the threat posed by countries of concern accessing government-related data or Americans' bulk U.S. sensitive personal data. As the President determined in the Order, ''[a]ccess to Americans' bulk sensitive personal data or United States Government-related data increases the ability of countries of concern to engage in a wide range of malicious activities.'' As the ANPRM explained, countries of concern can use their access to government-related data or Americans' bulk U.S. sensitive personal data to engage in malicious cyber-enabled activities and malign foreign influence activities and to track and build profiles on U.S. individuals, including members of the military and other Federal employees and contractors, for illicit purposes such as blackmail and espionage. And countries of concern can exploit their access to government-related data or Americans' bulk U.S. sensitive personal data to collect information on activists, academics, journalists, dissidents, political figures, or members of nongovernmental organizations or marginalized communities to intimidate them; curb political opposition; limit freedoms of expression, peaceful assembly, or association; or enable other forms of suppression of civil liberties.

As the 2024 National Counterintelligence Strategy explains, ''as part of a broader focus on data as a strategic resource, our adversaries are interested in personally identifiable information (PII) about U.S. citizens and others, such as biometric and genomic data, health care data, geolocation information, vehicle telemetry information, mobile device information, financial transaction data, and data on individuals' political affiliations and leanings, hobbies, and interests.'' [2] These and other kinds of sensitive personal data ''can be especially valuable, providing adversaries not only economic and [research and development] benefits, but also useful [counterintelligence] information, as hostile intelligence services can use vulnerabilities gleaned from such data to target and blackmail individuals.'' [3]

Nongovernmental experts have underscored these risks. For example, a recent study by the MITRE Corporation summarized open-source reporting, highlighting the threat of blackmail, coercion, identification of high-risk government personnel and sensitive locations, and improved targeting of offensive cyber operations and network exploitation posed by hostile actors' access to Americans' data derived from advertising technology.[4]

The development of artificial intelligence (''AI''), high-performance computing, big-data analytics, and other advanced technological capabilities by countries of concern amplifies the threat posed by these countries' access to government-related data or Americans' bulk U.S. sensitive personal data. For instance, the U.S. National Intelligence Council assessed in 2020 that ''access to personal data of other countries' citizens, along with [artificial intelligence]-driven analytics, will enable [the People's Republic of China] to automate the identification of individuals and groups beyond China's borders to target with propaganda or censorship.'' [5]

Countries of concern can also exploit their access to government-related data regardless of volume to threaten U.S. national security. One academic study explained that ''[f]oreign and malign actors could use location datasets to stalk or track high-profile military or political targets,'' revealing ''sensitive locations—such as visits to a place of worship, a gambling venue, a health clinic, or a gay bar—which again could be used for profiling, coercion, blackmail, or other purposes.'' [6] The MITRE report further explained that location datasets could reveal ''U.S. military bases and undisclosed intelligence sites'' or ''be used to

[2] Nat'l Counterintel. & Sec. Ctr., *National Counterintelligence Strategy 2024* 13 (Aug. 1, 2024), *https://www.dni.gov/files/NCSC/documents/features/NCSC_CI_Strategy-pages-20240730.pdf* [*https://perma.cc/9L2T-VXSU*].

[3] *Id.*

[4] Kirsten Hazelrig, Ser. No. 14, *Intelligence After Next: Surveillance Technologies Are Imbedded Into the Fabric of Modern Life—The Intelligence Community Must Respond,* The MITRE Corporation 2 (Jan. 5, 2023), *https://www.mitre.org/sites/default/files/2023-01/PR-22-4107-INTELLIGENCE-AFTER-NEXT-14-January-2023.pdf* [*https://perma.cc/3WA2-PGM2*].

[5] Nat'l Intel. Council, *Assessment: Cyber Operations Enabling Expansive Digital Authoritarianism* 4 (Apr. 7, 2020), *https://www.dni.gov/files/ODNI/documents/assessments/NICM-Declassified-Cyber-Operations-Enabling-Expansive-Digital-Authoritarianism-20200407-2022.pdf* [*https://perma.cc/ZKJ4-TBU6*].

[6] Justin Sherman et al., Duke Sanford Sch. of Pub. Pol'y, *Data Brokers and the Sale of Data on U.S. Military Personnel* 15 (Nov. 2023), *https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/11/Sherman-et-al-2023-Data-Brokers-and-the-Sale-of-Data-on-US-Military-Personnel.pdf* [*https://perma.cc/BBJ9-44UH*].

estimate military population or troop buildup in specific areas around the world or even identify areas of off-base congregation to target.'' [7] As another example of these data risks and the relative ease with which they can be exploited, journalists were able to commercially acquire from a data broker a continuous stream of 3.6 billion geolocation data points that were lawfully collected on millions of people from advertising IDs.[8] The journalists were then able to create ''movement profiles'' for tens of thousands of national security and military officials, and from there, could determine where they lived and worked as well as their names, education levels, family situations, and hobbies.[9]

The Order and this proposed rule seek to mitigate these and other national security threats that arise from countries of concern accessing government-related data or Americans' bulk U.S. sensitive personal data.

No current Federal legislation or rule categorically prohibits or imposes security requirements to prevent U.S. persons from providing countries of concern or covered persons access to sensitive personal data or government-related data through data brokerage, vendor, employment, or investment agreements. For example, the scope and structure of the Protecting Americans' Data from Foreign Adversaries Act of 2024 (*see* Pub. L. 118–50, div. I, 118th Cong. (2024)) do not create a comprehensive regulatory scheme that adequately and categorically addresses these national security risks, as explained in part IV.K of this preamble. Likewise, the Committee on Foreign Investment in the United States (''CFIUS'') has authority to assess the potential national security risks of certain investments by foreign persons in certain United States businesses that ''maintain[] or collect[] sensitive personal data of United States citizens that may be exploited in a manner that threatens national security.'' [10] CFIUS only reviews certain types of investments in U.S. businesses; it does so on a transaction-by-transaction basis, instead of prescribing prospective and categorical rules regulating all such transactions; and its authorities do not extend to other activities that countries of concern may use to gain access to government-related data or Americans' bulk U.S. sensitive personal data, such as through purchases of such data on the commercial market or through vendor or employment agreements.[11]

Similarly, Executive Order 13873 prohibits any acquisition, importation, transfer, installation, dealing in or use of by U.S. persons from acquiring certain information and communication technologies and services (''ICTS'') designed, developed, manufactured, or supplied by foreign adversaries where, among other things, the Secretary of Commerce determines that the transaction poses an ''unacceptable risk to the national security of the United States or the security and safety of United States persons.'' [12] In building upon the national emergency declared in Executive Order 13873, the President, in Executive Order 14034, determined that connected software applications operating on U.S. ICTS ''can access and capture vast swaths of . . . personal information and proprietary business information,'' a practice that ''threatens to provide foreign adversaries with access to that information.'' [13] However, as with CFIUS legal authorities, the orders do not broadly empower the United States Government to prohibit or otherwise restrict the sale of government-related data or Americans' bulk U.S. sensitive personal data, and the orders do not broadly restrict other commercial transactions, such as investment, employment, or vendor agreements, that may provide countries of concern access to government-related data or Americans' bulk U.S. sensitive personal data.

The proposed rule would complement these statutory and regulatory authorities. It prescribes forward-looking, categorical rules that prevent U.S. persons from providing countries of concern or covered persons access to government-related data or Americans' bulk U.S. sensitive personal data through commercial data-brokerage transactions. The proposed rule also imposes security requirements on other kinds of commercial transactions, such as investment, employment, and vendor agreements, that involve government-related data or Americans' bulk U.S. sensitive personal data to mitigate the risk that a country of concern could access such data. The proposed rule would address risks to government-related data or Americans' bulk U.S. sensitive personal data that current authorities leave vulnerable to access and exploitation by countries of concern and provide predictability and regulatory certainty by prescribing categorical rules regulating certain kinds of data transactions that could give countries of concern or covered persons access to government-related data or Americans' bulk U.S. sensitive personal data.

III. Advance Notice of Proposed Rulemaking and Comments

The National Security Division of the Department published an ANPRM on March 5, 2024 (former RIN: 1105–AB72), soliciting public comment on various topics related to the Order.[14] The Department received and carefully reviewed 64 timely comments in response to the ANPRM from trade associations, public interest advocacy groups, think tanks, private individuals, and companies, as well as comments from several foreign governments. The Department also received two additional ex parte comments after the comment period closed, which DOJ publicly posted on *regulations.gov.*

During the comment period, the Department of Justice, both on its own and with other agencies, met with businesses, trade groups, and other stakeholders potentially interested in or impacted by the contemplated regulations to discuss the ANPRM. For example, the Department discussed the ANPRM with the Consumer Technology Association, the Information Industry Technology Council, Pharmaceutical Research and Manufacturers of America, the Biotechnology Innovation Organization, the Bioeconomy Information Sharing Analysis Center, the U.S. Chamber of Commerce, Tesla, Workday, Anthropic, and the Special Competitive Studies Project, and it provided briefings to the Secretary of Commerce and Industry Trade Advisory Committees 6, 10, and 12 administered by the Office of the U.S. Trade Representative and the Department of Commerce. The Department also discussed the Order and contemplated regulations with stakeholders at events open to the public, including ones hosted by the American Conference Institute, the American Bar Association, the Center for Strategic and International Studies, and the R Street Institute, and through other public engagements such as the Lawfare Podcast, ChinaTalk Podcast, CyberLaw Podcast, and the Center for

[7] *Id.*

[8] Suzanne Smalley, *US Company's Geolocation Data Transaction Draws Intense Scrutiny in Germany,* The Record (July 18, 2024), *https://therecord.media/germany-geolocation-us-data-broker* [*https://perma.cc/ME9F-TAQ7*] (citing joint reporting by the German public broadcaster Bayerische Rundfunk and digital civil rights opinion news site *netzpolitik.org*).

[9] *Id.*

[10] 50 U.S.C. 4565(a)(4)(B)(iii)(III).

[11] *See generally* Foreign Investment Risk Review Modernization Act of 2018, Public Law 115–232, tit. XVII, secs. 1701–28, 132 Stat. 1636, 2173.

[12] E.O. 13873 of May 15, 2019, 84 FR 22689, 22690 (May 15, 2019).

[13] E.O. 14034, 86 FR 31423, 31423 (June 9, 2021).

[14] 89 FR 15780 (Mar. 5, 2024).

Cybersecurity Policy & Law's Distilling Cyber Policy podcast.

After the comment period closed, the Department of Justice, along with the Department of Commerce, followed up with commenters who provided feedback regarding the bulk thresholds to discuss that topic in more detail, including the Council on Government Relations Industry Association, Association of American Medical Colleges, Airlines for America, Bank Policy Institute, the Business Roundtable, Information Technology Industry Council, Centre for Information Policy Leadership, Biotechnology Innovation Organization, Software and Information Industry Association, Cellular Telephone Industries Association, the internet and Television Association, US Telecom, Ford Motor Company, Bioeconomy Information Sharing and Analysis Center, Coalition of Services Industries, Enterprise Cloud Coalition, Electronic Privacy Information Center, Center for Democracy and Technology, Business Software Alliance, Global Data Alliance, Interactive Advertising Bureau, U.S.-China Business Council, IBM, Workday, and individuals Justin Sherman, Mark Febrizio, and Charlie Lorthioir. The Department has also discussed the Order and the ANPRM with foreign partners to ensure that they understood the Order and contemplated program and how they fit into broader national security, economic, and trade policies.

The Department considered each comment submitted, including the ex parte comments that have since been publicly posted. Many of the comments were general in nature and supported the Department's efforts and approach with respect to the proposed rule. Overall, commenters were generally supportive of the intent of the proposed rule. However, several commentators representing industry questioned the effectiveness of the proposed rule as compared to the passage of a holistic federal privacy law, proposed revisions, and highlighted areas where the proposed rule would benefit from further clarity. The Department discusses comments, and any edits or revisions made in response to the comments, in the discussion of the proposed rule in part IV of this preamble.

IV. Discussion of the Proposed Rule

The proposed rule implements the Order through categorical rules that regulate certain data transactions involving government-related data or bulk U.S. sensitive personal data that could give countries of concern or covered persons access or the ability to access such data and present an unacceptable risk to U.S. national security. The proposed rule (1) identifies certain classes of highly sensitive transactions with countries of concern or covered persons that the proposed rule would prohibit in their entirety (''prohibited transactions'') and (2) identifies other classes of transactions that would be prohibited except to the extent they comply with predefined security requirements (''restricted transactions'') to mitigate the risk of access to bulk U.S. sensitive personal data by countries of concern. The Attorney General has determined that the prohibited and restricted transactions set forth in the proposed rule pose an unacceptable risk to the national security of the United States because they may enable countries of concern or covered persons to access and exploit government-related data or bulk U.S. sensitive personal data.

In addition to identifying classes of prohibited and restricted transactions that pose an unacceptable risk to national security, the proposed rule identifies certain classes of transactions that are exempt from the proposed rule. For example, the proposed rule exempts transactions for the conduct of the official business of the United States Government by employees, grantees, or contractors thereof, and transactions conducted pursuant to a grant, contract, or other agreement entered into with the United States Government, including those for outbreak and pandemic prevention, preparedness, and response. The proposed rule also defines relevant terms; identifies countries of concern; defines covered persons; and creates processes for the Department to issue general and specific licenses, to issue advisory opinions, and to designate entities or individuals as covered persons. The proposed rule also establishes a compliance and enforcement regime.

The Department relied upon unclassified and classified sources to support the proposed rule. Although the unclassified record fully and independently supports the proposed rule without the need to rely on the classified record, the classified record provides supplemental information that lends additional support to the proposed rule. The proposed rule would be the same even without the classified record.

Some commenters offered overarching comments. A few commenters made suggestions that addressed issues unrelated to the proposed rule, such as expressing views on U.S. positions in certain international negotiations over digital trade. No change was made in response to these comments. These comments addressed unrelated issues that are not relevant to the scope of the proposed rule and that are directed to other agencies and forums, and they generally did not suggest any specific changes to the contemplated program. To the extent that these comments intended to suggest that the Order's and proposed rule's restrictions on access to sensitive personal data are inconsistent with international commitments by the United States, the Department disagrees.

The proposed rule's prohibitions and restrictions on access to U.S. sensitive personal data and government-related data by countries of concern are consistent with access restrictions on sensitive personal data that have long been imposed in other national security contexts, including for some transactions reviewed by CFIUS and the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (''Team Telecom'').[15] Those access restrictions, in turn, are consistent with or otherwise permissible under trade and other international agreements.[16] For example, the World Trade Organization's (''WTO'') General Agreement on Trade in Services (''GATS''), like other trade agreements to which the United States is a party, includes an essential security interests exception that states that nothing in the agreement shall be construed to prevent a party to such an agreement from taking any action that it considers necessary for the protection of its essential security interests. As a result, rather than prohibiting such access restrictions, GATS and other relevant international agreements to which the United States is a party explicitly authorize national security-based restrictions on data access and data flows through the longstanding essential security exception. The proposed rule, like conditions restricting access in CFIUS or Team Telecom mitigation

[15] *See* Foreign Investment Risk Review Modernization Act of 2018, supra note 11 (CFIUS); E.O. 13913, 85 FR 19643 (Apr. 4, 2020) (Team Telecom); *see, e.g.,* FCC, New Pacific Light Cable Network GU Holdings-Google National Security Agreement 20–044 Enclosure 1 (Dec. 16, 2021), *https://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/related_filing.hts?f_key=-448225&f_number=SCLLIC2020082700038* [*https://perma.cc/PD5E-BYWS*].

[16] *See, e.g.,* Agreement on Trade-Related Aspects of Intellectual Property Rights art. 73, Apr. 15, 1994, amended Jan. 23, 2017, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299, *https://www.wto.org/english/docs_e/legal_e/31bis_trips_09_e.htm* [*https://perma.cc/FSP4-BBZQ*]; General Agreement on Tariffs and Trade art. XXI, Oct. 30, 1947, 61 Stat. A—11, 55 U.N.T.S. 194, *https://www.wto.org/english/docs_e/legal_e/31bis_trips_e.pdf* [*https://perma.cc/LE7M-ZM4F*].

agreements to address identified national security risks, is necessary to protect the essential security interests of the United States and is thus consistent with such international agreements to which the United States is a party.[17] Notably, consistent with the United States Government's long-standing support of cross-border data flows, the proposed rule does not require data localization or wholly restrict data flows to any specific country. Rather, the proposed rule only limits data transfers in narrow, specifically defined circumstances necessary to safeguard security interests, and it is being developed through a process that enables stakeholder consultation and input. The proposed rule is also consistent with the United States' longstanding support for Data Free Flows Trust (''DFFT''). The categories of prohibited and restricted transactions in the proposed rule identify circumstances that present an unacceptable national security risk of enabling countries of concern to access and exploit Americans' sensitive personal data—circumstances that lack the trust required for free data flows.

Several commenters suggested various revisions to borrow or incorporate aspects of international or State privacy laws into this proposed rule. The Department generally declines to adopt these suggestions, except on a discrete issue discussed in part IV.A.7 of this preamble. The Department supports privacy measures and national security measures as complementary protections for Americans' sensitive personal data. Despite some overlap, privacy protections and national security measures generally focus on different challenges associated with sensitive personal data. General privacy protections focus on addressing individual rights and preventing individual harm, such as protecting the rights of individuals to control the use of their own data and reducing the potential harm to individuals by minimizing the collection of data on the front end and limiting the permissible uses of that data on the back end. National security measures, by contrast, focus on collective risks and externalities that may result from how individuals and businesses choose to sell and use their data, including in lawful and legitimate ways.

For example, some commenters suggested adding a new exemption for transactions in which a U.S. individual consents to the sale or disclosure of their data to a country of concern or covered person. The proposed rule declines to adopt this exemption. Such a consent-based exemption would leave unaddressed the threat to national security by allowing U.S. individuals and companies to choose to share government-related data or Americans' bulk U.S. sensitive personal data with countries of concern or covered persons. It is precisely those choices that, in aggregate, help create the national security risk of access by countries of concern or covered persons, and the purpose of the Order and the proposed rule is to address the negative externality that is created by individuals' and companies' choices in the market in the first place. It would also be inconsistent with other national security regulations to leave it up to market choices to decide whether to give American technology, capital, or data to a country of concern or covered person. Export controls do not allow U.S. companies to determine whether their sensitive technology can be sent to a foreign adversary, and sanctions do not allow U.S. persons to determine whether their capital and material support can be given to terrorists and other malicious actors. Likewise, the proposed rule would not allow U.S. individuals to determine whether to give countries of concern or covered persons access to their sensitive personal data or government-related data. One of the reasons that the public is not in a position to assess and make decisions about the national security interests of the United States is that the public typically does not have all of the information available to make a fully informed decision about the national security interests of the United States.

Each subpart of the proposed rule, including any relevant comments received on the corresponding part of the ANPRM, is discussed below in the remaining sections of this preamble.

A. Subpart C—Prohibited Transactions and Related Activities

The proposed rule identifies transactions that are categorically prohibited unless the proposed rule otherwise authorizes them pursuant to an exemption or a general or specific license or, for the categories of restricted transactions, in compliance with security requirements and other requirements set forth in the proposed rule.

1. Section 202.210—Covered Data Transactions

The Order authorizes the Attorney General to issue regulations that prohibit or otherwise restrict U.S. persons from engaging in a transaction where, among other things, the Attorney General has determined that a transaction ''is a member of a class of transactions . . . [that] pose an unacceptable risk to the national security of the United States because the transactions may enable countries of concern or covered persons to access bulk sensitive personal data or United States Government-related data in a manner that contributes to the national emergency declared in this [O]rder.'' [18] Pursuant to the Order, the proposed rule categorically prohibits or, for the categories of restricted transactions, imposes security and other requirements on certain covered data transactions with U.S. persons and countries of concern or covered persons because the covered data transactions may otherwise enable countries of concern or covered persons to access government-related data or bulk U.S. sensitive personal data to harm U.S. national security.

The proposed rule defines a ''covered data transaction'' as any transaction that involves any access 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. *See* § 202.210. The Department has determined that these categories of covered data transactions pose an unacceptable risk to U.S. national security because they may enable countries of concern or covered persons to access government-related data or bulk U.S. sensitive personal data to engage in malicious cyber-enabled activities, track and build profiles on United States individuals for illicit purposes, including blackmail or espionage, and to intimidate, curb political dissent or political opposition, or otherwise limit civil liberties of U.S. persons opposed to countries of concern, among other harms to U.S. national security. For instance, one study has demonstrated that foreign malign actors can purchase bulk quantities of sensitive personal data about U.S. military personnel from data brokers ''for coercion, reputational damage, and blackmail.'' [19] Countries of

[17] *See* Press Release, Off. of the U.S. Trade Representative, *Statements by the United States at the Meeting of the WTO Dispute Settlement Body* (Jan. 27, 2023), *https://ustr.gov/about-us/policy-offices/press-office/press-releases/2023/january/statements-united-states-meeting-wto-dispute-settlement-body* [*https://perma.cc/CQG5-9AZ5*] (emphasizing the United States' commitment to protect its essential security interests in the context of World Trade Organization disputes); General Agreement on Tariffs and Trade art. XXI, *supra* note 16.

[18] 89 FR 15423.

[19] Justin Sherman et al., *supra* note 6, at 14.

concern or covered persons could also exploit vendor, employment, or investment agreements to obtain access to government-related data or bulk U.S. sensitive personal data to harm U.S. national security.[20]

In response to the ANPRM, commenters asked that the Department clarify when a transaction ''involves'' government-related data or bulk U.S. sensitive personal data. The Department has responded to those comments by revising the definition of a ''covered data transaction'' to any transaction that involves any access to the data by the counterparty to a transaction (rather than any transaction that involves government-related data or bulk U.S. sensitive personal data).

2. Section 202.301—Prohibited Data-Brokerage Transactions

The proposed rule prohibits any U.S. person from knowingly engaging in a covered data transaction involving data brokerage with a country of concern or a covered person. The proposed rule defines ''data brokerage'' as the sale of data, licensing of access to data, or similar commercial transactions 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. *See* § 202.214.

Because the data brokerage prohibition, along with the other prohibitions and restrictions, center around data transactions involving access to government-related data or bulk U.S. sensitive personal data, the Department addresses each of those key terms and related terms in detail in the following discussion.

3. Section 202.201—Access

Adopting the approach contemplated in the ANPRM without change, the proposed rule defines ''access'' as 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.

One commenter suggested that the Department remove the term ''divert'' from the definition of ''access'' to avoid unintentionally capturing activities that do not involve actual access to data and that, according to the commenter, do not pose a risk to national security. The Department declines to do so. The definition of ''access'' is intentionally broad. It includes the term ''divert'' to ensure that the proposed rule covers data transactions that would enable a covered person to divert government-related data or bulk U.S. sensitive personal data from an intended recipient to a country of concern or a covered person, either for their own use or for the use of countries of concern or other covered persons, and to prevent countries of concern or covered persons from amassing data (including anonymized, encrypted, aggregated, or pseudonymized data), as discussed in part IV.A.13 of this preamble.

4. Section 202.249—Sensitive Personal Data

As previewed in the ANPRM, the proposed rule builds on the Order by further defining the six categories of ''sensitive personal data'' that could be exploited by a country of concern to harm U.S. national security if that data is linked or linkable to any identifiable U.S. individual or to a discrete and identifiable group of U.S. persons. These six categories are: (1) covered personal identifiers; (2) precise geolocation data; (3) biometric identifiers; (4) human genomic data; (5) personal health data; and (6) personal financial data. The proposed rule also categorically excludes certain categories of data from the definition of the term ''sensitive personal data.'' These exclusions include public or nonpublic data that does not relate to an individual, including trade secrets and proprietary information, and data that is, at the time of the transaction, lawfully publicly available from government records or widely distributed media, personal communications as defined in § 202.239, and information or informational materials as defined in § 202.226. Nothing in the proposed rule shall be construed to affect the obligations of U.S. Government departments and agencies under the Foundations for Evidence-Based Policymaking Act of 2018, Public Law 115–435 (2019), 44 U.S.C. 3501 *et seq.*

5. Section 202.212—Covered Personal Identifiers

The Order defines ''covered personal identifiers'' as ''specifically listed classes of personally identifiable data that are reasonably linked to an individual, and that—whether in combination with each other, with other sensitive personal data, or with other data that is disclosed by a transacting party pursuant to the transaction and that makes the personally identifiable data exploitable by a country of concern—could be used to identify an individual from a data set or link data across multiple data sets to an individual,'' subject to certain exclusions.[21] The ANPRM thus contemplated three subcategories of covered personal identifiers: (1) listed identifiers in combination with any other listed identifier; (2) listed identifiers in combination with other sensitive personal data; and (3) listed identifiers in combination with other data that are disclosed by a transacting party pursuant to the transaction that makes the listed identifier exploitable by a country of concern, if they could be used to identify an individual from a dataset or to link data across multiple datasets to an individual.[22] The ANPRM also contemplated two exceptions: (1) demographic or contact data that is linked only to other demographic or contact data; and (2) a network-based identifier, account-authentication data, or call-detail data that is linked only to other network-based identifiers, account-authentication data, or call-detail data as necessary for the provision of telecommunications, networking, or similar services. The proposed rule expands the approach described in the ANPRM by making the exceptions applicable to all subcategories of covered personal identifiers, instead of being applicable only to listed identifiers in combination with any other listed identifiers. The listed identifiers are described in more detail in the next section.

With respect to the first subcategory, listed identifiers in combination with any other listed identifier: The ANPRM contemplated a list-based approach that would identify a comprehensive list of eight classes of data determined by the Attorney General to be reasonably linked to an individual under the Order's definition of ''covered personal identifiers.'' [23]

With respect to the second subcategory, listed identifiers in combination with other sensitive

[20] *See, e.g.,* Dep't of Commerce, Final Determination: Case No. ICTS–20121–002, Kaspersky Lab, Inc., 89 FR 52434, 52436 (June 24, 2024), *https://www.govinfo.gov/content/pkg/FR-2024-06-24/pdf/2024-13532.pdf* [*https://perma.cc/LAS7-S7HF*] (describing how Kaspersky employees gained access to sensitive U.S. person data through their provision of anti-virus and cybersecurity software); *see generally* OFAC, U.S. Dep't of Treas., *Guidance on the Democratic People's Republic of Korea Information Technology Workers* (May 16, 2022), *https://ofac.treasury.gov/media/923131/download?inline* [*https://perma.cc/8DTV-Q34S*]; E.O. 14083, 87 FR 57369, 57373 (Sept. 15, 2022).

[21] E.O. 14117, 89 FR 15421,15428 (Feb 28, 2024).

[22] 89 FR 15784–85.

[23] *Id.*

personal data: The ANPRM contemplated treating these combinations as combined data subject to the lowest bulk threshold applicable to the categories of data present.[24] The proposed rule generally adopts the approach described in the ANPRM, but instead of addressing this category in the definition of ''listed identifiers,'' the proposed rule incorporates this category as part of the definition of ''bulk.''

With respect to the third subcategory, listed identifiers in combination with other data that are disclosed by a transacting party pursuant to the transaction that makes the listed identifier exploitable by a country of concern: The ANPRM indicated that the Department did not intend to impose an obligation on transacting parties to independently determine whether particular combinations of data would be ''exploitable by a country of concern.'' [25] The ANPRM provided several examples intended to be within the scope of this subcategory and several examples intended to be outside the scope of this subcategory and sought comment on ways in which this subcategory could be further defined.[26] In response, multiple commenters suggested anchoring this subcategory to the reasonable foreseeability that the other data could be used to link the listed identifier to a U.S. individual. As these commenters explained, without the connection to foreseeability, nearly any public data could become covered personal identifiers, because it is possible that the transacting party receiving the data could find some way of linking any public data point to an individual using the listed identifier.

The proposed rule largely adopts this suggestion. Rather than requiring companies to determine when linkage is reasonably foreseeable on a case-by-case basis, the proposed rule would define a category of data for which the Department believes it is reasonably foreseeable that the other data could be used to link the listed identifier to a U.S. individual: other data that makes the listed identifier linked or linkable to other listed identifiers or to other sensitive personal data. The proposed rule thus narrows the third subcategory to any listed identifier in combination with other data that is disclosed by a transacting party such that the listed identifier is linked or linkable to other listed identifiers or to other sensitive personal data. *See* § 202.212(a)(2). The proposed rule also incorporates the examples described in the ANPRM and additional examples to illustrate how this subcategory would and would not apply.

6. Section 202.234—Listed Identifier

Adopting the approach contemplated in the ANPRM,[27] the proposed rule defines a ''listed identifier'' as any piece of data in any of the following data fields: (1) 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); (2) full financial account numbers or personal identification numbers associated with a financial institution or financial-services company; (3) 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); (4) 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); (5) advertising identifier (such as Google Advertising ID, Apple ID for Advertisers, or other mobile advertising ID (''MAID'')); (6) account-authentication data (such as account username, account password, or an answer to a security question); (7) network-based identifier (such as internet Protocol (''IP'') address or cookie data); or (8) call-detail data (such as Customer Proprietary Network Information (''CPNI'')). *See* § 202.234.

Under this definition, the term ''covered personal identifiers'' refers to a much narrower set of material than that covered by certain laws and policies aimed generally at protecting personal privacy.[28] It encompasses only the types of data and combinations thereof that are expressly listed. For example, the proposed rule's definition of ''covered personal identifiers'' would not include an individual's employment history, educational history, organizational memberships, criminal history, or web-browsing history. Some commenters suggested that the Department adopt a broader definition that aligns with the definition of ''personally identifiable information'' used in State or European Union (''EU'') privacy laws to ease the burden of compliance. The Department declines to adopt this approach, and the proposed rule retains the definition stated in the ANPRM without change. Although it may be true that ''personally identifiable information'' is a familiar term in laws and guidance addressing the privacy and security of data held by the private sector and government, it is such a broad term that adopting a definition akin to it would significantly expand the scope of the regulations and therefore require that the Department regulate more commercial transactions or relationships than seem necessary, at least at this time, to mitigate the highest priority national security risks articulated in the Order. Furthermore, the commenters supplied no data to suggest that any cost savings realized from adopting an existing definition would outweigh the added burdens of regulating a larger swath of transactions.

Similarly, another commenter suggested broadening the definition of ''covered personal identifiers'' to add categories of data from State and EU privacy laws, such as web-browsing data and data that identifies or could lead to inferences about membership in protected classes such as race, religion, and national origin. The proposed rule makes no change in response to this comment. As previewed in the ANPRM, the proposed rule's definition of ''covered personal identifiers'' is tailored to address the national security risks identified in the Order, and the Department is establishing the program by issuing proposed rulemakings in tranches based on priority. Also, the Department intends to regularly monitor the effectiveness and impact of the regulations once they become effective. Absent more specific information from commenters on this topic about the cross-border use of these additional kinds of identifiers by foreign governments in ways that could harm Americans, the proposed rule retains the definition stated in the ANPRM without change at this time.

One commenter suggested that the Department remove basic contact information from the listed identifiers. The proposed rule maintains the approach in the ANPRM without change.[29] The Order already contains an exception to the definition of ''covered personal identifiers'' for demographic or contact data that is linked only to other demographic or contact data. The proposed rule implements the exception articulated in the Order and previewed

[24] *Id.* at 15785.

[25] *Id.*

[26] *Id.*

[27] *Id.* at 15784.

[28] *C.f., e.g.,* California Consumer Privacy Act of 2018, Cal. Civ. Code sec. 1798.140(v)(1) (West 2024) (defining ''personal information'' in the context of a generalized privacy-focused regime); Regulation (EU) 2016/679 of the European Parliament and of the Council of Apr. 27, 2016, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, art. 4(1) (defining ''personal data'' in the context of a generalized data privacy regime).

[29] 89 FR 15784.

in the ANPRM, which excludes such data from the definition of ''covered personal identifiers.'' [30]

By contrast, another commenter recommended that ''covered personal identifiers'' be expanded to include demographic or contact data that is linked only to other demographic or contact data, because most Americans believe that information to be deserving of privacy protections. The Department declines to adopt this addition to the definition of ''covered personal identifiers.'' Such an expansion of the definition would be contrary to the Order, which specifically exempts this kind of data from its scope.[31] Additionally, as the commenter acknowledges, a significant amount of this information is already publicly available to countries of concern, and therefore country of concern access to this type of information does not carry the same national security risk as access to the other covered personal identifiers identified in these regulations, even if it may raise separate privacy considerations.

A few commenters advocated removing truncated government identification and account numbers from the definition of ''listed identifiers,'' given their widescale use. One commenter supported the inclusion of these truncated identifiers because they are regularly used to identify individuals. The proposed rule continues to include these truncated identifiers as contemplated in the ANPRM because, as one commenter points out, they could be, and are, ''used to identify an individual from a data set or link data across multiple data sets to an individual[.]'' They therefore fall within the Order's definition of ''covered personal identifiers'' when they are combined with certain other categories of data. Although these truncated numbers may be used widely, the proposed rule would not regulate how they are used in most transactions. Specifically, it would not regulate how these truncated numbers are used domestically, a company's internal use of that data (other than with respect to covered persons who are employees), or transactions abroad involving third countries (other than with respect to certain conditions for the data brokerage to address onward sale).

The proposed rule also contains a non-substantive change in language designed to be more technically accurate and to clarify that any piece of data in any of the listed classes of data constitutes a listed identifier. *See* § 202.234. This change remains consistent with the examples previewed in the ANPRM and in the proposed rule showing that multiple pieces of data (such as account username and account password) in the same data field (account-authentication data) each count as separate listed identifiers.[32]

7. Section 202.242—Precise Geolocation Data

The proposed rule defines ''precise geolocation data'' as 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. Examples of ''precise geolocation data'' include GPS coordinates and IP address geolocation. To help develop this definition, the Department examined the settings available to software developers in Android and iOS, the two most popular mobile device operating systems, for the precision of geolocation readings. Available options included accuracy to within 10 meters, 100 meters, 1,000 meters, 3,000 meters, and 10,000+ meters.[33] The Department selected 1,000 meters as the option that most carefully balanced the risk that countries of concern or covered persons could exploit U.S. persons' precise geolocation data and current technology practices and standards. The Department also considered State privacy laws, with which companies are already familiar and which provide examples of the level of precision at which a device's location warrants protection.[34]

A few commenters suggested that the Department define ''precise geolocation data'' as that term is defined in the California Privacy Rights Act, which includes a geographic radius of 1,850 feet (approximately 563 meters). The Department did not accept this suggestion because our assessment of the relevant national security interests required a broader geographic area, in part due to the types of United States Government personnel and locations (such as military bases with large surrounding footprints) that are relevant to national security. By contrast, the California standard does not take these national security interests relating to Government personnel into account. One commenter suggested that the Department omit the phrase ''based on electronic signals or inertial sensing units,'' which was included in the ANPRM definition of ''precise geolocation data,'' to make the term more technology-neutral as to the method of collection.[35] The Department has adopted this suggestion and deleted that phrase from the proposed definition.

8. Section 202.204—Biometric Identifiers

Adopting the approach contemplated in the ANPRM without change, the proposed rule defines ''biometric identifiers'' as 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.

9. Section 202.224—Human Genomic Data

Adopting the approach contemplated in the ANPRM without change, the proposed rule defines ''human genomic data'' as 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. The term ''human genomic data'' does not include non-human data, such as pathogen genetic sequence data, that is derived from or integrated into human genomic data.

10. Other Human 'Omic Data

The Department of Justice is considering regulating, as prohibited or restricted transactions in the final rule, certain transactions in which a U.S. person provides a country of concern (or covered person) with access to bulk human 'omic data, other than human genomic data, as defined in § 202.224. At a high level, the 'omics sciences examine biological processes that contribute to the form and function of cells and tissues.[36] The categories of 'omic data that the Department is considering regulating could include

[30] *Id.*

[31] 89 FR 15428.

[32] 89 FR 15785.

[33] *CLLocationAccuracy,* Apple Developer, *https://developer.apple.com/documentation/corelocation/cllocationaccuracy* [*https://perma.cc/AZ48-VSCP*]; *Change Location Settings,* Android Developer, *https://developer.android.com/develop/sensors-and-location/location/change-location-settings* [*https://perma.cc/5BY3-P7L3*].

[34] *See, e.g.,* Cal. Civ. Code sec. 1798.140(w) (which uses a radius of 1,850 feet); Utah Consumer Privacy Act, Utah Code Ann. sec. 13–61–101(33)(a) (West 2024) (which uses a radius of 1,750 feet).

[35] 89 FR 15785.

[36] *See, e.g., Evolution of Translational Omics: Lessons Learned and the Path Forward* 23, 33 (Christine M. Micheel et al., eds., 2012), *https://www.ncbi.nlm.nih.gov/books/NBK202168/pdf/Bookshelf_NBK202168.pdf* [*https://perma.cc/Q5YE-7XLM*].

human epigenomic data, glycomic data, lipidomic data, metabolomic data, meta-multiomic data, microbiomic data, phenomic data, proteomic data, and transcriptomic data. The Department does not intend the definition of meta-multiomic data to include nonhuman data separated from human data or for the definition of microbiomics data to include data related to individual pathogens, even when derived from human sources. The Department is considering whether to include the following definitions of these terms in the final rule:

1. Epigenomic data: data derived from the analysis of human epigenetic modifications, which are changes in gene expression or cellular phenotype 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.

2. Glycomic data: data derived from the analysis of the structure, function, and interactions of glycans (complex carbohydrates) within human biological systems. The field of glycomics generally aims to understand the roles of glycans in cell–cell communication, immune responses, and various diseases.

3. Lipidomic data: data derived from a systems-level characterization of lipids from a human or human cell, including their identification, quantification, and characterization in biological systems. Routine clinical measurements of lipids for individualized patient care purposes would not be considered lipidomic data because such measurements would not entail a systems-level analysis of the complete set of lipids found in such a sample.

4. Metabolomic data: data derived from the analysis of metabolites, the small molecules produced during metabolism, that aim to understand disease mechanisms, identify biomarkers for diagnosis, and develop targeted treatments by revealing the dynamic biochemical activities in a living system. This data provides a general snapshot of an organism, tissue, or cell, offering insights into physiological and pathological processes.

5. Meta-multiomic data: The Department is considering the following options for defining meta-multiomic data:

(i) Datasets that include two or more categories of human 'omic data identified in this regulation, which can include data derived from the human genome, proteome, transcriptome, epigenome, or metabolome; or

(ii) Datasets that include two or more categories of human 'omic data identified in this regulation and that include 'omic data from another species.

6. Microbiomic data: data derived from analysis of all the microorganisms of a given community within the human body (including a particular site on the human body). Microbiomic data is implicated in the field of metagenomics, which generally aims to investigate and understand genetic material of entire communities of organisms, including the composition of a microbial community.

7. Phenomic data: data derived from analysis of human phenotypes, including physical traits, physiological parameters, and behavioral characteristics.

8. Proteomic data: data derived from analysis of human proteomes, which refers to the entire set of proteins expressed by a human genome, cell, tissue, or organism. The field of proteomics generally aims to identify and characterize proteins and study their structures, functions, interactions, and post-translational modifications.

9. Transcriptomic data: data derived from analysis of a human transcriptome, which is the complete set of RNA transcripts produced by the human genome under specific conditions or in a specific cell type. The field of transcriptomics generally aims to understand gene expression patterns, alternative splicing, and regulation of RNA molecules.

The Department is considering excluding from the definition of other human 'omic data pathogen-specific data embedded in 'omic data sets.

The Department welcomes input from commenters regarding the potential risks and benefits that may arise from restricting or prohibiting covered data transactions with a country of concern or covered person involving some or all of these categories of other human 'omic data. The Department is particularly interested in comments addressing the health, economic, or scientific impacts of regulating such data transactions, as well as any national security implications. Specifically:

- In what ways, if any, should the Department of Justice elaborate or amend the definitions of these classes of other human 'omic data? If the definitions should be elaborated or amended, why?
- Should bulk data transactions involving these types of other human 'omic data be regulated? If so, which types of human 'omic data—including any not listed—should be regulated, why should they be regulated, and how should they be regulated? Additionally, what bulk thresholds should apply and why?
- To what extent would the regulation of bulk data transactions involving these types of other human 'omic data affect individuals' rights to share their own biological samples (*e.g.,* blood, urine, tissue, etc.) or health, 'omic, and other data?
- What would be the effects of prohibiting or restricting transactions involving these data classes in the final rule, particularly with respect to:
  - health outcomes
  - health supply chain impacts
  - research and administrative costs
  - economic costs due to (1) imposing these regulations, or (2) allowing unregulated bulk access to human 'omic data
  - innovation costs
- What additional risks should be considered if these bulk data transactions are not regulated, specifically as they relate to:
  - risks stemming from exploitable health information
  - manipulation of bulk data for strategic advantage over the United States
  - use of bulk datasets for the creation and refinement of AI or other similar advanced technologies

11. Section 202.240—Personal Financial Data

Adopting the approach contemplated in the ANPRM without change, the proposed rule defines ''personal financial data'' as data about an individual's credit, charge, or debit card, or bank account, including purchases and payment history; data, including assets liabilities, debts, and transactions in a bank, credit, or other financial statement; or data in a credit report or in a ''consumer report'' (as defined in 15 U.S.C. 1681a(d)).

One commenter sought clarification that personal financial data does not include inferences based on that data, suggesting, for example, that hotel record transactions may be personal financial data but an ultimate inference that the person is interested in business travel should not be considered personal financial data. As set forth in the Order and previewed in the ANPRM, the proposed rule would prohibit or restrict only certain categories of transactions in government-related data or bulk U.S. sensitive personal data, neither of which include inferences on their own.[37]

[37] 89 FR 15783; 89 FR 15428–29.

12. Section 202.241—Personal Health Data

The ANPRM contemplated defining ''personal health data'' as ''individually identifiable health information,'' as defined under the Health Insurance Portability and Accountability Act of 1996 (''HIPAA''), ''regardless of whether such information is collected by a 'covered entity' or 'business associate.' '' [38]

Several commenters supported defining personal health data as ''individually identifiable health information.'' That definition is similar to how those terms are defined in HIPAA and its implementing regulations. However, one commenter expressed confusion as to how cross-referencing that definition in this program would relate to ''covered entities'' or ''business associates'' under HIPAA. The proposed rule adopts much of the substance of the approach in the ANPRM while providing greater clarity to address this confusion. Instead of defining ''personal health information'' by cross referencing and incorporating HIPAA, the proposed rule reproduces the relevant substance of the HIPAA definition to provide greater clarity that the definition does not turn on the HIPAA-specific inquiry of whether data is handled by covered entities or business associates. Further, unlike the HIPAA definition, the proposed rule would not define health information in terms of whether the information identifies individuals, because the proposed rule applies regardless of whether data is de-identified.

As a result, the proposed rule defines ''personal health data'' as health information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual. The 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. The proposed rule would operate on a categorical basis and would determine that the category of personal health data generally meets the requirements of being ''exploitable by a country of concern to harm United States national security'' and ''is linked or linkable to any identifiable United States individual or to a discrete and identifiable group of United States individuals'' under section 7(l) of the Order. To be sure, it is possible to hypothesize a limited data set of discrete information related to an individual's physical or mental health condition that is not inherently linked or linkable to U.S. individuals (such as a data set of only heights or weights with no identifying information). But based on the information currently available, it does not appear that such limited datasets accurately reflect how personal health data is stored, transmitted, and used in the real world, and thus it does not appear appropriate to adjust the proposed rule to account for this hypothetical at this time. The Department welcomes comments on the extent to which such datasets exist and are the subject of covered data transactions between U.S. persons and countries of concern or covered persons.

13. Section 202.206—Bulk U.S. Sensitive Personal Data

Adopting the approach contemplated in the ANPRM without change, the prohibitions and restrictions apply to ''bulk U.S. sensitive personal data,'' which the proposed rule defines as 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. The bulk thresholds of data set by the proposed rule are addressed in detail in part V of this preamble.

Several commenters requested that the Department align the categories of sensitive personal data with State data privacy laws, particularly to exclude encrypted, pseudonymized, de-identified, or aggregated data from the proposed rule's coverage. In contrast, other commenters supported the Department's treatment of pseudonymized, de-identified, or encrypted data, including to prevent the data from being re-identified in the future and to recognize that not all techniques for pseudonymization, de-identification, encryption, or aggregation are equally effective. The Department declines to adjust the proposed rule to exclude anonymized, encrypted, pseudonymized, or de-identified data, and the proposed rule adopts the approach described in the ANPRM without change. As the Order emphasizes, even where types of sensitive personal data are ''anonymized, pseudonymized, or de-identified, advances in technology, combined with access by countries of concern to large datasets, increasingly enable countries of concern that access this data to re-identify or de-anonymize data,'' which could reveal exploitable sensitive personal information on U.S. persons.[39] As the Department has recently explained, ''[o]pen-source reporting has repeatedly raised concern[s] that supposedly anonymized data is rarely, if ever, truly anonymous.'' [40] As a recent study has explained, for example, ''[a]ggregated insights from location data'' could be used to damage national security.[41] Examples abound. Researchers in 2024 used a little more than a year's worth of ''raw, 'ping'-level data, a year's worth of location data from de-identified smartphones in 26 major metropolitan areas encompassing nearly every SEC office and most public firm headquarters to identify non-public investigations and enforcement actions, and glean insights about how those visits affected financial markets.[42] In 2018, the publication of a global heatmap of anonymized users' location data collected by a popular fitness app enabled researchers to quickly identify and map the locations of military and government facilities and activities.[43] Similarly, in 2019, *New York Times* writers were able to combine a single set of bulk location data collected from cell phones and bought and sold by location-data companies—which was anonymized and represented ''just one slice of data, sourced from one company, focused on one city, covering less than one year''—with publicly available information to identify, track, and follow ''military officials with security clearances as they drove home at night,'' ''law enforcement officers as they took their kids to school,'' and ''lawyers (and their guests) as they

[38] *Id.; see* 42 U.S.C. 1320d(6); 45 CFR 160, 103.

[39] 89 FR 15426; *see also* E.O. 14083, 87 FR 57369, 57372–73 (Sept. 15, 2022).

[40] *In Camera, Ex Parte* Classified Decl. of David Newman, Principal Deputy Assistant Att'y Gen., Nat'l Sec. Div., U.S. Dep't of Just., Doc. No. 2066897 at Gov't App. 74–75 ¶¶ 100–01, *TikTok Inc.* v. *Garland,* Case Nos. 24–1113, 24–1130, 24–1183 (D.C. Cir. July 26, 2024) (publicly filed redacted version) (hereinafter ''Newman Decl.'').

[41] Sherman et al., *supra* note 6, at 15.

[42] William C. Gerken et al., *Watching the Watchdogs: Tracking SEC Inquiries using Geolocation Data* 2–4 (Aug. 30, 2024) (unpublished manuscript), *https://ssrn.com/abstract=4941708* [*https://perma.cc/L7L9-WU3T*].

[43] *E.g.,* Richard Perez-Pena & Matthew Rosenberg, *Strava Fitness App Can Reveal Military Sites, Analysts Say,* N.Y. Times (Jan. 29, 2018), *https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html* [*https://perma.cc/FT3A-W547*]; Jeremy Hsu, *The Strava Heat Map and the End of Secrets,* Wired (Jan. 29, 2018), *https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/* [*https://perma.cc/6TWD-P76B*].

traveled from private jets to vacation properties.'' [44] A 2019 research study concluded that ''99.98% of Americans would be correctly re-identified in any dataset using 15 demographic attributes,'' thus ''suggest[ing] that even heavily sampled anonymized datasets are unlikely to satisfy the modern standards for anonymization set forth by [the EU's General Data Protection Regime] and seriously challenge the technical and legal adequacy of the de-identification release-and-forget model.'' [45] Other studies and reports have reported similar results.[46] As a result, as the Department recently explained, ''[a]dversaries can use these datasets to reverse-engineer anonymized data and identify people, subjects, or devices that were supposedly anonymized.'' [47]

Similar concerns exist with respect to encrypted data. Countries of concern amass large quantities of encrypted data including by harvesting encrypted data now in order to decrypt it in the future should advances in quantum technologies render current standard public-key cryptographic algorithms ineffective.[48] Encryption keys can also be stolen, handed over under compulsion, and otherwise obtained for use in decrypting datasets.[49]

A few commenters suggested that the approach contemplated in the ANPRM would weaken national security by failing to differentiate between data that is encrypted or otherwise protected and data that is not. In their view, encryption is an important tool to secure data from unauthorized access, and treating encrypted and non-encrypted data alike could discourage the use of encryption, weakening the overall security of data. Other commenters, however, supported treating pseudonymized, encrypted, de-identified, and aggregated data as sensitive personal data because of the ability to re-identify such data and the rapid advancements in re-identification techniques. The Department declines to modify the proposed rule in response to these comments. As contemplated in the ANPRM, the proposed rule explicitly recognizes and relies upon the privacy and national security-preserving value of high quality, effective methods of encryption, de-identification, pseudonymization, and aggregation by specifically authorizing certain otherwise prohibited transactions so long as they meet the security requirements described in part IV.B.1 of this preamble, including by using data-level control(s) such as these techniques in combination with other security requirements. At the same time, as contemplated in the ANPRM, the proposed rule also recognizes that ineffective methods of encryption, de-identification, pseudonymization, and aggregation present the same unacceptable national security risk of access by countries of concern and covered persons as the risks posed by such access to identifiable data that is not secured through any of these techniques. The proposed rule thus allows otherwise prohibited employment agreements, vendor agreements, and investment agreements only if they use any combination of the data-level requirements necessary to prevent access to covered data by covered persons or countries of concern, as requirements laid out in the security requirements to be published by the Department of Homeland Security (''DHS''), in addition to organizational- and system-level requirements.

Commenters also requested that the Department use existing State privacy law definitions to define the categories of sensitive personal data, such as personal financial data. Commenters stated that many companies already know how to comply with State privacy laws. The Department has considered these comments. However, as discussed in part IV.A.6 of this preamble, the cited definitions do not necessarily align with the specific national security goals of these regulations. Therefore, the proposed rule adopts the approach described in the ANPRM without change and does not adopt the State privacy law definitions of the terms in the proposed rule.

14. Section 202.205—Bulk

As previewed in the ANPRM, the proposed rule's prohibitions apply to bulk amounts of U.S. sensitive personal data (in addition to the separate category of government-related data). The proposed rule defines ''bulk'' as any amount of such data that meets or exceeds thresholds during a given 12-month period, whether through one covered data transaction or multiple covered data transactions involving the same U.S. person and the same foreign person or covered person. The proposed rule sets specific thresholds for each category of sensitive personal data. *See* § 202.205. Certain specified data transactions that exceed those thresholds are ''covered data transactions'' and thus subject to the proposed rule's prohibitions unless they are otherwise authorized by the proposed rule. *See* § 202.210. The Department has determined the proposed bulk thresholds based on the analysis previewed in the ANPRM and described in more detail in part V of this preamble.

A few commenters expressed concerns that it would be necessary to decrypt data to determine whether it meets a relevant bulk threshold and suggested discarding the bulk thresholds as a result. They noted that decrypting data is generally less secure and could lead to unauthorized access. The proposed rule makes no change in response to these comments, for several reasons. First, many businesses engaging in the categories of prohibited and restricted transactions generally use

[44] Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy,* N.Y. Times (Dec. 19, 2019), *https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html* [*https://perma.cc/X3VB-429P*].

[45] Luc Rocher et al., *Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models,* 10 Nature Commc'ns, at 1 (2019), *https://www.nature.com/articles/s41467-019-10933-3.pdf* [*https://perma.cc/SYJ7-KA95*]; *see also* Alex Hern, *'Anonymised' Data Can Never Be Totally Anonymous, Says Study,* The Guardian (Jul. 23, 2019), *https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds* [*https://perma.cc/5BF8-745A*].

[46] *See, e.g.,* Alex Hern, *New York Taxi Details Can Be Extracted From Anonymised Data, Researchers Say,* The Guardian (June 27, 2014), *https://www.theguardian.com/technology/2014/jun/27/new-york-taxi-details-anonymised-data-researchers-warn* [*https://perma.cc/6SYK-6ZEG*] (reporting that a researcher ''discovered that the anonymous data'' of taxi records ''was easy to restore to its original, personally identifiable format,'' taking a ''matter of only minutes to determine which [license] numbers were associated with which pieces of anonymised data'' and only an hour to ''de-anonymise the entire dataset,'' making it possible to ''figure out which person drove each trip'' and to determine taxi drivers' supposedly anonymous home addresses); Ryan Singel, *Netflix Spilled Your Brokeback Mountain Secret, Lawsuit Claims,* Wired (Dec. 17, 2009), *https://www.wired.com/2009/12/netflix-privacy-lawsuit/* [*https://perma.cc/B96P-AY97*] (reporting on researchers who de-anonymized a Netflix dataset of movie ratings by using publicly available information, which revealed ''political leanings and sexual orientation'' in some cases, and reporters who ''quickly'' de-anonymized supposedly anonymous AOL search-engine logs ''to track down real people'').

[47] Newman Decl., *supra* note 40, at Gov't App. 33 ¶ 105.

[48] David Lague, *U.S. and China Race to Shield Secrets from Quantum Computers,* Reuters (Dec. 14, 2023), *https://www.reuters.com/investigates/special-report/us-china-tech-quantum/* [*https://perma.cc/9HAA-46XA*]; Nat'l Counterintel. & Sec. Ctr., *Protecting Critical and Emerging U.S. Technologies From Foreign Threats* 5 (Oct. 2021), *https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_Emerging%20Technologies_Factsheet_10_22_2021.pdf* [*https://perma.cc/L6ZU-8HU7*]; Nat'l Cybersec. Ctr. of Excellence, NIST SP 1800–38B, *Migration to Post-Quantum Cryptography,* at 1 (drft. Dec. 2023), *https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf* [*https://perma.cc/FXF2-BJ62*].

[49] *Can Encrypted Data be Hacked?,* IT Foundations (Apr. 19, 2021), *https://itfoundations.com/can-encrypted-data-be-hacked/* [*https://perma.cc/E3TN-YAVV*].

the data in the course of operating their business, rather than merely serving as a pass-through for encrypted data as the comments suggest. While encrypting data in transit and data at rest is and should be a standard security technique, and encrypting data in use is increasingly common, data is routinely decrypted while it is being actively accessed, processed, filtered, sorted, searched, analyzed, displayed, and otherwise used by a business (for example, when an authorized employee or user opens and searches an encrypted file or database). However, nothing in the proposed rule imposes a legal requirement to decrypt data to comply. Instead, the proposed rule requires only that U.S. persons implement a risk-based compliance program tailored to their individual risk profiles. And data may also be encrypted using cryptographic methods that permit some computation and analysis to be performed on cyphertext that ascertains the kinds and volume of data without decrypting the data.[50] Businesses can map the kinds and volumes of their data to evaluate it against the bulk thresholds in the data life cycle in which it is either decrypted for access or encrypted in use.

Second, even beyond mapping data in use, companies choosing to engage in these categories of data transactions can and should have some awareness of the volume of data they possess and in which they are transacting. For example, typically data-using entities maintain metrics, such as user statistics, that can help estimate the number of impacted individuals for the purposes of identifying whether a particular transaction meets the bulk threshold.[51] Given that the bulk thresholds are built around order-of-magnitude evaluations of the quantity of user data, it is reasonable for entities to conduct similar order-of-magnitude-based assessments of their data stores and transactions for the purposes of regulatory compliance. Companies already must understand, categorize, and map the volumes of data they have for other regulatory requirements, such as State laws requiring notification of data breaches of specific kinds of data above certain thresholds.[52]

Third, this concern appears premised on a scenario in which a U.S. business handles only encrypted data on which no computational functions can be performed to determine the kinds and volume of data, never accesses the decrypted data in its business, does not have other proxies or metrics to determine the kinds and volumes of data in which it is transacting, and must comply with the prohibitions and restrictions in the proposed rule. This scenario appears to be an edge case at best, and the comments do not provide a real-world example of this scenario or its frequency. Indeed, as discussed in some of the examples contained in the proposed rule, if a U.S. entity merely provides a platform for, or transports data between, a U.S. customer and a covered person or country of concern, and thus does not know or reasonably should not know of the kind or volume of data involved, then it generally would not ''knowingly'' engage in a prohibited transaction if the U.S. customer uses that platform or infrastructure to engage in a prohibited transaction with a covered person. Instead, the U.S. customer would generally be responsible for having ''knowingly'' engaged in the prohibited transaction, as illustrated in the clarification of the ''knowingly'' standard and the new examples incorporated into the proposed rule. *See* § 202.230. Similarly, if a U.S. entity merely stores encrypted data on behalf of a U.S. customer and does not possess the encryption key, and if the U.S. entity does not know or reasonably should not know the kind or volume of data involved, the U.S. entity generally would not meet the ''knowingly'' standard of the proposed rule.

Fourth, to the extent that there is a U.S. business that handles only encrypted data on which no computational functions can be performed to determine the kinds and volume of data, never accesses the decrypted data in its business, does not have other proxies or metrics to determine the kinds and volumes of data it is transacting, and is subject to the prohibitions and restrictions in the proposed rule, that U.S. business would have choices under the proposed rule. It would be able to engage with the Department and seek an advisory opinion or a specific license tailored to its business. Similarly, it would have choices about how best to comply as part of its individualized, risk-based compliance program. For example, it can choose not to engage in prohibited or restricted transactions with countries of concern or covered persons as part of its individualized risk-based compliance program. If the U.S. business chooses to engage in categories of transactions potentially subject to the proposed rule, it can conduct reasonable due diligence on the source of its encrypted data (such as engaging with and obtaining contractual commitments from its customers) to determine the volume and kinds of data in which it is transacting. Or, if it chooses to engage in restricted transactions with countries of concern or covered persons, it can assume that its transactions involve bulk volumes of sensitive personal data and comply with the security requirements and other applicable conditions out of an abundance of caution.

Even if this hypothetical U.S. business were to choose to engage in categories of transactions potentially subject to the proposed rule, and it voluntarily decided to briefly decrypt the data to determine the kinds and volume of its data as part of its risk-based compliance program, commentors have not provided evidence that such a brief decryption would meaningfully increase the risks of unauthorized access relative to the risks involved in routine decryption for business use. Encryption is one security tool designed to mitigate the risk of unauthorized access to data.[53] Entities should use encryption as a tool whenever possible, including when data is at rest, in transit, and in use. However, using encryption does not eliminate risk or the requirement to perform appropriate due diligence. If an entity is using data at any point or has access to both encrypted data and the encryption key, that entity has full se into and control over the data on its systems for the

[50] Abbas Acar et al., *A Survey on Homomorphic Encryption Schemes: Theory and Implementation,* 51 [No. 4] ACM Computing Survs. 79:1, 79:2 (2018), *https://dl.acm.org/doi/pdf/10.1145/3214303* [*https://perma.cc/AM69-7ZWV*]. In addition, to the extent that businesses use emerging techniques (such as homomorphic encryption) that permit computations to be performed on encrypted data without first decrypting it, these techniques may enable businesses to map their data even if it remains encrypted.

[51] Justin Ellingwood, *User Data Collection: Balancing Business Needs and User Privacy,* DigitalOcean (Sept. 26, 2017), *https://www.digitalocean.com/community/tutorials/user-data-collection-balancing-business-needs-and-user-privacy* [*https://perma.cc/GCX5-RGSK*]; Jodie Siganto, *Data Tagging: Best Practices, Security & Implementation Tips,* Privacy108 (Nov. 14, 2023), *https://privacy108.com.au/insights/data-tagging-for-security/* [*https://perma.cc/8PQA-89DA*]; National Institutes of Health, *Metrics for Data Repositories and Knowledgebases: Working Group Report* 7, (Sept. 15, 2021), *https://datascience.nih.gov/sites/default/files/Metrics-Report-2021-Sep15-508.pdf* [*https://perma.cc/8KBQ-HWRK*].

[52] *See, e.g.,* Del. Code. Ann. tit. 6, sec. 12B—100 to—104 (West 2024); N.M. Stat. Ann. sec. 57–12C–10 (LexisNexis 2024).

[53] *What Is Encryption?,* Cloudflare, *https://www.cloudflare.com/learning/ssl/what-is-encryption/* [*https://perma.cc/T3KT-BURX*]; Cybersec. & Infrastructure Sec. Agency, *Zero Trust Maturity Model* 5, 27 (v. 2.0 Apr. 2023), *https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf* [*https://perma.cc/F9LB-JVL9*].

purposes of this regulation.[54] Entities are responsible for balancing risks within their systems, with encryption serving as one available tool for achieving risk management goals alongside other tools like data governance and data minimization plans, role-based and least-privilege access controls, and identity management through multifactor authentication.[55]

It is the responsibility of the regulated entity to manage risk that already exists, which includes making choices about the best way to manage its own particular risk and tradeoffs between various data risk management strategies, including technical measures like encryption, organizational policies, and access management. Other options include altering commercial activities to minimize the size and scope of covered data transactions and utilizing a strong data governance regime to minimize the type and quantity of data collected. If data cannot remain encrypted while in use, the risk of temporarily decrypting data to comply with regulations can be offset by measures such as well-designed data collection, data management, and data security programs. Given these factors, any risk associated with a hypothetical U.S. business' decision to temporarily decrypt data that would otherwise remain encrypted at all times in the business' life cycle would appear to be much more remote and attenuated than the risk that accrues by allowing the U.S. business to engage in a transaction that grants a country of concern or covered person access to encrypted government-related data or bulk U.S. sensitive personal data.

15. Section 202.222—Government-Related Data

As set forth in § 202.222, the proposed rule would not impose any bulk threshold requirements on transactions involving government-related data. The proposed rule defines subcategories of government-related data for locations and personnel, as contemplated in the ANPRM. For the location subcategory, the proposed rule defines ''government-related data'' as any precise geolocation data, regardless of volume, for any location within any area enumerated on the Government-Related Location Data List in § 202.1401 that the Attorney General has determined poses a heightened risk of being exploited by a country of concern to reveal insights to the detriment of national security about locations controlled by the Federal Government, including insights about facilities, activities, or populations in those locations, because of the nature of those locations or the personnel who work there. The purpose of this list is to prevent countries of concern from exploiting the geolocation data in these locations, such as by using aggregated geolocation data to draw inferences about facilities, activities, or populations located there that could undermine U.S. national security or foreign policy or to conduct intelligence or counterintelligence operations against government employees or contractors, or against government facilities, as discussed in parts II, IV(D) and V(A) of this preamble. As set forth in the proposed rule, the locations that the Department might add to this list may include the worksites or duty stations of Federal Government employees or contractors who occupy national security positions, as that term is defined in 5 CFR 1400.102(a), wherever they are located. The locations may also include military installations, embassies or consulates, or other facilities worldwide that support the Federal Government in achieving its national security, defense, intelligence, law enforcement, or foreign policy missions. The proposed rule thus modifies the definition contemplated in the ANPRM by setting forth more details about the types of locations that will be listed on the Government-Related Location Data List.[56]

The proposed rule also proposes a format for the Government-Related Location Data List and proposes some areas for inclusion on that List. *See* § 202.1401. This is not yet a comprehensive list of locations. The Department anticipates that the final rule will include additional locations associated with military, other Government, or other sensitive facilities or locations that meet the criteria in the definition. These locations may include, for example, military bases, embassies, or law enforcement facilities.

For the personnel subcategory, the proposed rule adopts the ANPRM's contemplated definition without change by defining ''government-related data'' as 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.[57]

Commenters were generally supportive of the proposed rule's protections for government-related data. A few commenters requested that the proposed rule provide clarity as to what constitutes a ''former senior official'' and a ''recent former employee.'' The proposed rule defines ''recent former employees or contractors'' as employees or contractors who have worked for or provided services to the United States Government, in a paid or unpaid status, within the 2 years preceding a proposed covered data transaction. *See* § 202.245. The proposed rule defines a ''former senior official'' as either a ''former senior employee'' or ''former very senior employee,'' as those terms are defined in the ethics regulations pertaining to post-employment conflicts of interest for former Executive Branch or independent agency employees. 5 CFR 2641.104. *See* § 202.220.

One commenter expressed concern that, with respect to the personnel subcategory, companies will have to ask individuals whether they are former government employees when collecting their data and retain that information to ensure they can comply with the regulations. The commenter argued that this could have the unintended consequence of inadvertently creating a database of sensitive information that bad actors could target. While the Department appreciates that concern and agrees that this unintended consequence should be avoided, the Department has designed the proposed rule to specifically avoid this problem by defining the personnel subcategory based on how the U.S. person markets the data, not on whether a particular dataset contains data on former government employees or contractors. In other words, the personnel subcategory applies only to transactions in which the U.S. person has already identified and described sensitive personal data as being about certain government personnel. This subcategory does not apply on the basis of the presence or absence of data linked to

[54] Clare Stouffer, *What Is Encryption? How It Works + Types of Encryption,* Norton: Blog (July 18, 2023), *https://us.norton.com/blog/privacy/what-is-encryption* [*https://perma.cc/RC3D-NS95*].

[55] Nat'l Sec. Agency & Cybersec. & Infrastructure Sec. Agency, *Recommended Best Practices for Administrators: Identity and Access Management* (n.d.), *https://media.defense.gov/2023/Mar/21/2003183448/-1/-1/0/ESF%20identity%20and%20access%20management%20recommended%20best%20practices%20for%20administrators%20pp-23-0248_508c.pdf* [*https://perma.cc/B7VP-4RWF*]; Mohammed Khan, *Data Minimization—A Practical Approach,* ISACA (Mar. 29, 2021), *https://www.isaca.org/resources/news-and-trends/industry-news/2021/data-minimization-a-practical-approach* [*https://perma.cc/8APH-5E5A*]; Cybersec. & Infrastructure Sec. Agency, *Protecting Sensitive and Personal Information From Ransomware-Caused Data Breaches* (n.d.), *https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Protecting_Sensitive_and_Personal_Information_from_Ransomware-Caused_Data_Breaches-508C.pdf* [*https://perma.cc/Q7TN-NLR4*].

[56] 89 FR 15787.

[57] *Id.*

certain government personnel in the underlying sensitive personal data.

One commenter suggested removing the qualifier that data had to be ''marketed'' as data about members of the military or intelligence community because certain data can still be ''linked or linkable'' to members of the military through geolocation without being explicitly marketed as such. As the Order's second category of government-related data confirms, sensitive personal data that is linked to categories of data that could be used to identify current or certain former government personnel can present a national security risk, even if a transacting party does not market it as linked or linkable to those personnel.[58] The Department is still considering how to address this issue, specifically whether to include, and how to define, this category of information in the proposed rule while minimizing the unintended consequence described above in this section. The Department appreciates any views from the public.

16. Section 202.302—Other Prohibited Data-Brokerage Transactions Involving Potential Onward Transfer to Countries of Concern or Covered Persons

As previewed in the ANPRM, the proposed rule also includes a prohibition specific to data brokerage to address transactions involving the onward transfer or resale of government-related data or bulk U.S. sensitive personal data to countries of concern and covered persons.[59] *See* § 202.302. The proposed rule defines ''data brokerage'' as the sale of data, licensing of access to data, or similar commercial transactions 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. *See* § 202.214. The proposed rule prohibits any U.S. person from knowingly engaging in a covered data transaction involving data brokerage with any foreign person that is not a covered person unless the U.S. person contractually requires that the foreign person refrain from engaging in a subsequent covered data transaction involving that data with a country of concern or covered person. This narrow circumstance is the only instance in which the proposed rule's regulation of covered data transactions could impact transactions involving third countries (*i.e.,* U.S. persons' covered data transactions in which a country of concern or covered person is not a party).

Commenters generally supported the feasibility of using contractual requirements to address the resale of data as contemplated in the ANPRM. They noted, however, that it may be difficult for U.S. persons to enforce those requirements or to ensure that the data is not subsequently resold in violation of those provisions. Several aspects of the proposed rule are designed to address these concerns. First, in addition to requiring a contractual commitment from the foreign person not to engage in a subsequent covered data transaction with a country of concern or covered person, as contemplated in the ANPRM, the proposed rule adds a requirement for U.S. persons engaged in such transactions to report any known or suspected violations of the required contractual provision. This requirement creates a mechanism to provide the necessary information for the Department to investigate and take appropriate action to address any violations of the proposed rule. Second, relying on both its own investigations and its investigations of any known or suspected violations reported by private parties, the Department intends to exercise the designation authority under the proposed rule to designate as covered persons, as appropriate, foreign third parties that violate the contractual provisions required by this prohibition. *See* § 202.701. Third, consistent with the overall approach to compliance and enforcement under the proposed rule, the Department expects U.S. persons engaged in these kinds of data brokerage transactions to take reasonable steps to evaluate whether their foreign counterparties are complying with the contractual provision as part of implementing risk-based compliance programs under the proposed rule. Absent indications of evasion, conspiracy, or knowingly directing prohibited transactions, U.S. persons that conduct adequate due diligence as part of a risk-based compliance program would not have engaged in a prohibited transaction if the foreign counterparty later violates the required contractual provision or if the U.S. person fails to detect such violations. Depending on the circumstances, a U.S. person's failure to conduct adequate due diligence may subject the U.S. person to enforcement actions if that failure would constitute an evasion of the regulations, such as repeatedly knowing of violations by a foreign person and continuing to engage in data-brokerage transactions with that foreign person. The Department welcomes public input on any additional measures that should be considered as part of the final rule. In addition, after the final rule goes into effect, the Department intends to monitor the effectiveness of the measures to address the risk of onward sale and make any appropriate adjustments.

Although not specifically raised by commenters, the Department is considering the specific language used to describe the contractual requirement. As previewed in the ANPRM,[60] the proposed rule frames the contractual requirement as an obligation to provide that the foreign party ''refrain from engaging in a subsequent covered data transaction involving the same data with a country of concern or covered person.'' *See* § 202.302(a)(1). The Department invites public comment on this language, including whether any alternative language (such as inserting ''knowingly'' before ''refrain'' or ''contractually requires that the foreign person use best efforts not to engage'') would be more appropriate.

Commenters expressed varying views about the contemplated definition of ''data brokerage.'' Several commenters expressed concerns about the breadth of the definition of ''data brokerage'' in the ANPRM.[61] Some commenters suggested that the proposed term, and in particular the phrase ''or similar commercial transactions,'' creates uncertainty as to its scope and fails to distinguish between selling data for monetary purposes and transferring data pursuant to normal business operations. Some commenters urged the Department to limit the scope of the proposed rule to ''data brokers'' by adopting the definition used in existing State privacy laws, such as California's.[62] Others proposed ways that the Department should narrow the definition, including by requiring that the data be sold in exchange for monetary or other valuable consideration; that the data must be the object of the transaction and not shared incident to the development, testing, or sale of a product or service; or that the data must be knowingly transferred or sold. Other commenters suggested that the Department amend the definition of ''sale'' to exclude the disclosure of sensitive personal data to service providers processing data on behalf of a U.S. company, to third parties for providing products or services requested by a U.S. company, or for

[58] 89 FR 15429.

[59] 89 FR 15792.

[60] *Id.*

[61] *See* 89 FR 15788.

[62] *See* Cal. Civ. Code 1798.99.80 (West 2024).

disclosures or transfers to subsidiaries or affiliates of U.S. companies. Still other commenters supported the approach contemplated by the ANPRM for defining data brokerage by reference to transactions, not the identities of the parties, noting that the ANPRM's approach is stronger than existing State privacy laws, and encouraged the adoption of a broad definition.

The Department declines to revise the definition of ''data brokerage'' in response to these comments. The definition of ''data brokerage'' in the proposed rule is intentionally designed to address the activity of data brokerage that gives rise to the national security risk, regardless of the kind of entity that engages in it. Both first-party data brokerage (*i.e.,* by the person that directly collected the U.S. person's data) and third-party data brokerage (*i.e.,* by a person that did not directly collect the U.S. person's data, such as a subsequent reseller) present similar national security risks: the outright sale and transfer of sensitive personal data to a country of concern or covered person. For this reason, the proposed definition intentionally regulates data transactions, including transactions that transfer data to entities in countries of concern for product development, an issue raised by numerous commenters, because those transactions give rise to the risks discussed in the Order. In addition, commenters did not provide any specific evidence that the proposed definition of data brokerage would have any measurable economic impact related to product development or testing.[63] Consequently, the proposed rule maintains the approach described in the ANPRM without change.

A few commenters expressed concern about how this provision might affect the ability of biomedical and pharmaceutical manufacturers to share clinical trial data with drug and device regulators in countries of concern. Relatedly, a few commenters expressed concerns that the proposed rule's inclusion of aggregated and anonymized data would prohibit companies from using clinical trial data to launch clinical trials in countries of concern or sharing safety and efficacy data obtained from clinical trials in the United States with countries of concern. The proposed rule includes two exemptions responsive to these comments, in sections 202.510 and 202.511. These exemptions allow certain transactions relevant to medical research, marketing, and safety, as explained in more detail below.

[63] *See infra* note 418 and accompanying text.

17. Section 202.303—Prohibited Human Genomic Data and Human Biospecimen Transactions

As previewed in the ANPRM, the proposed rule includes a prohibition to specifically address the risks posed by covered data transactions involving access by countries of concern to U.S. persons' bulk human genomic data and human biospecimens from which that bulk data can be derived, such as covered data transactions that give access to bulk human genomic data to laboratories owned or operated by covered persons or provide them with human biospecimens from which such data can be derived. The proposed rule prohibits any U.S. person from knowingly engaging in any covered data transaction involving human genomic data that provides a country of concern or covered person with access to bulk U.S. sensitive personal data that consists of human genomic data or human biospecimens from which such data could be derived, where the number of U.S. persons in the dataset is greater than the applicable bulk threshold at any point in the preceding 12 months, whether in a single covered data transaction or aggregated across covered data transactions. This prohibition applies to any of the categories of covered data transactions that involve access to bulk human genomic data or human biospecimens from which bulk human genomic data can be derived, even when the transactions involve an employment, investment, or vendor agreement. In other words, transactions falling within the scope of proposed § 202.303 are never treated as restricted transactions under the proposed rule. Relatedly, and as discussed in more detail with respect to the categories of exempt transactions, the proposed rule exempts (1) transactions for the conduct of the official business of the United States Government by employees, grantees, or contractors thereof, or transactions conducted pursuant to a grant, contract, or other agreement entered into with the United States Government, including those for outbreak and pandemic prevention, preparedness, and response; and (2) data transactions, including the sharing of human biospecimens from which human genomic data may be derived, that are required or authorized by certain specified international arrangements addressing global and pandemic preparedness.

One commenter sought clarification that vendor, employment, and investment agreements involving access to bulk human genomic data, or human biospecimens from which such data could be derived, are prohibited transactions under subpart C of the proposed rule rather than restricted transactions under subpart D of the proposed rule. The commenter suggested that the proposed rule should clarify that such vendor, employment, and investment agreements are prohibited because they present the same policy concerns as other categories of transactions involving access to this kind of data. The Department agrees. As shown by Example 49 in the ANPRM, vendor, employment, and investment agreements involving access to this kind of sensitive personal data are prohibited rather than restricted.[64] For the avoidance of doubt, § 202.303 of the proposed rule clarifies that the authorization for restricted transactions, *see* §§ 202.401–202.402, does not apply to any transactions involving access to bulk human genomic data or bulk human biospecimens.

18. Section 202.304—Prohibited Evasions, Attempts, Causing Violations, and Conspiracies

Adopting the approach contemplated in the ANPRM without change, the proposed rule prohibits any transactions that have the purpose of evading or avoiding the proposed rule's prohibitions, or that cause a violation of or attempt to violate the proposed rule's prohibitions. The proposed rule also prohibits conspiracies formed to violate the proposed rule's prohibitions.

One commenter suggested expanding the scope of the regulations to prohibit transactions involving algorithms or artificial intelligence models that are trained and developed using bulk U.S. sensitive personal data in certain circumstances. The commenter described a scenario in which the transfer of such an algorithm or model provides a means to evade the prohibitions—for example, where a transaction gives a country of concern or covered person access to the model, and the model makes the underlying bulk U.S. sensitive personal data on which it was trained available to that country of concern or covered person. According to the commenter, this access could occur by querying the model in such a way that results in it sharing all of or a highly relevant component of the underlying data on which it was trained, such as a query that resulted in identification of people with a particular medical condition.[65] Apart

[64] 89 FR 15794.

[65] Tim Johansson & Balder Janryd, Preventing Health Data from Leaking in a Machine Learning System 4–6 (2024) (First Cycle 15 credits, KTH Royal Institute of Technology), *https://kth.diva-*

Continued

from concerns over access to the underlying data, a model could also provide insights into counter-intelligence targeting that would not otherwise be observable from the underlying sensitive personal data. The Department shares these concerns. In response to the comment, the proposed rule includes Examples 5 and 6 in § 202.304(b) highlighting how these regulations would apply in certain scenarios where bulk U.S. sensitive personal data would be licensed or sold to support algorithmic development, including cases of evasion, or where sensitive personal data could be extracted from artificial intelligence models. The Department will continue to evaluate the national-security risks in this emerging area as it considers the effectiveness of this regulation. To the extent that there are broader concerns about national-security risks from the export of artificial intelligence models or algorithms regardless of the access they provide to sensitive personal data (such as their ability to provide insights that would not otherwise be observable from the data on which they are trained), the Department believes that other authorities, such as export controls and Executive Order 13859 of February 11, 2019 (Maintaining American Leadership in Artificial Intelligence),[66] are more appropriate in the first instance to address those concerns.

19. Section 202.305—Knowingly Directing Prohibited Transactions

Adopting the approach contemplated in the ANPRM without change, the proposed rule prohibits U.S. persons from knowingly directing any covered data transaction that would be a prohibited transaction (including restricted transactions that do not comply with the security requirements) if engaged in by a U.S. person.

20. Section 202.215—Directing

Adopting the approach contemplated in the ANPRM without change, the proposed rule defines ''directing'' to mean that the U.S. person has any authority (individually or as part of a group) to make decisions on behalf of a foreign entity and exercises that authority. For example, a U.S. person would direct a transaction by exercising their authority to order, decide to engage, or approve a transaction that would be prohibited under these regulations if engaged in by a U.S. person.

21. Section 202.230—Knowingly

Adopting the approach contemplated in the ANPRM without change, the proposed rule defines ''knowingly'' to mean, with respect to conduct, a circumstance, or a result, that the U.S. person had actual knowledge of, or reasonably should have known about, the conduct, circumstance, or result. To determine what an individual or entity reasonably should have known in the context of prohibited transactions, the Department will take into account the relevant facts and circumstances, including the relative sophistication of the individual or entity at issue, the scale and sensitivity of the data involved, and the extent to which the parties to the transaction at issue appear to have been aware of and sought to evade the application of these proposed rules. As a result of the knowledge standard, the regulations incorporating the word ''knowingly'' do not adopt a strict liability standard.

The ''knowingly'' language is also not intended to require U.S. persons, in engaging in vendor agreements and other classes of data transactions with foreign persons, to conduct due diligence on the employment practices of those foreign persons to determine whether the foreign persons' employees qualify as covered persons. For instance, as illustrated by Examples 37 and 38 in the ANPRM, which are incorporated into the proposed rule, it would not be a prohibited transaction for a U.S. person to enter into a vendor agreement to have bulk U.S. sensitive personal data processed or stored by a foreign person that is not a covered person, even if that foreign person then employs covered persons and grants them access to the data (absent any indication of evasion or knowing direction).[67] In those circumstances, the U.S. person would not be expected to conduct due diligence on the foreign person's employment practices as part of its risk-based compliance program.

Several commenters sought clarity about liability where service providers have little or no knowledge of the data that customers keep or transact on their infrastructure. They also requested that the Department distinguish between data controllers and data processers. In response to these comments, the proposed rule has provided additional examples to clarify the function of the ''knowingly'' standard. *See* § 202.230(b)(2)–(6). As the examples demonstrate, if a U.S. entity merely provides a software platform or owns or operates infrastructure for a U.S. customer, and thus does not know or reasonably should not know of the kind or volume of data involved, then the U.S. entity generally would not ''knowingly'' engage in a prohibited transaction if the U.S. customer uses their platform or infrastructure to engage in a prohibited transaction. Instead, the U.S. customer would generally be responsible for having ''knowingly'' engaged in the prohibited transaction. Likewise, if a U.S. entity merely stores encrypted data on behalf of a U.S. customer and does not have access to the encryption key (or has access only to an emergency backup encryption key usable only at the customer's explicit request), and if the U.S. entity is reasonably unaware of the kind or volume of data involved, the U.S. entity generally would not meet the ''knowingly'' standard of the proposed rule.

The Department declines, however, to draw a categorical distinction between processors and controllers in the proposed rule. Inserting a categorical distinction based on the kind of entity would be inconsistent with the structure and overall approach of the proposed rule, which addresses activities that present an unacceptable national security risk. In addition, as the new examples illustrate, the same kinds of entities can engage in different kinds of activities, some of which (such as merely providing a software platform) raise different risks than others (such as providing a software platform and services to handle and process the data). The ''knowingly'' standard provides the requisite flexibility to address the national security risks while providing a basis to distinguish responsibility based on the activities and roles that particular entities may have. The proposed rule thus adopts the approach described in the ANPRM with the additional examples described above in this section to illustrate the ''knowingly'' standard.

Similarly, one comment sought clarification that the proposed rule would apply only to U.S. persons that have or maintain control over the bulk U.S. sensitive personal data involved in a prohibited or restricted transaction. As the commenter explained, an automobile manufacturer should not have compliance obligations with respect to bulk U.S. sensitive personal data that is transferred via an aftermarket device that was installed in a vehicle fleet by the owner. As

portal.org/smash/get/diva2:1865596/FULLTEXT01.pdf [*https://perma.cc/S5S8-M3DJ*]; *see, e.g.,* Anuj Mudaliar, *ChatGPT Leaks Sensitive User Data, OpenAI Suspects Hack,* Spiceworks (Feb. 1, 2024), *https://www.spiceworks.com/tech/artificial-intelligence/news/chatgpt-leaks-sensitive-user-data-openai-suspects-hack/* [*https://perma.cc/AS5E-FATZ*].

[66] E.O. 13859, 84 FR 3967 (Feb. 11, 2019).

[67] 89 FR 15792.

previewed in the ANPRM, the proposed rule imposes prohibitions and restrictions only on U.S. persons that are engaged in covered data transactions that meet certain criteria. In the commenter's example, the U.S. automobile manufacturer has not engaged in a covered data transaction with respect to the aftermarket device. As a result, no change was made to the proposed rule in response to this comment.

B. Subpart D—Restricted Transactions

1. Section 202.401—Authorization To Conduct Restricted Transactions; Section 202.402—Incorporation by Reference

The proposed rule sets forth three classes of transactions (vendor agreements, employment agreements, and investment agreements) that are prohibited unless the U.S. person entering into the transactions complies with the ''security requirements'' referenced in section 202.248. The goal of the proposed security requirements is to address national security and foreign-policy threats that arise when countries of concern and covered persons access government-related data or bulk U.S. sensitive personal data that may be implicated by the categories of restricted transactions. The security requirements have been developed and proposed by the Cybersecurity and Infrastructure Security Agency (''CISA'') in coordination with the Department. CISA has published the proposed requirements—the CISA Proposed Security Requirements for Restricted Transactions—on its website, as announced via a **Federal Register** notice requesting comment on those proposed security requirements issued concurrently with this proposed rule. The proposed security requirements require U.S. persons engaging in restricted transactions to comply with organizational and system-level requirements, such as ensuring that basic organizational cybersecurity policies, practices, and requirements are in place, as well as data-level requirements, such as data minimization and masking, encryption, or privacy-enhancing techniques. After CISA receives and considers public input, it will revise as appropriate and publish the final security requirements. The Department of Justice will then incorporate by reference the published final security requirements in the final rule that the Department issues. Interested parties can view CISA's proposed security requirements on CISA's website at *https://www.cisa.gov/* and can review CISA's notice requesting comments on the proposed security requirements in the notice docketed as CISA–2024–0029 (October 29, 2024).

The proposed rule also clarifies that restricted transactions are not prohibited only if they comply with the security requirements and other applicable requirements for conducting restricted transactions. The proposed rule includes a new example that makes it clear that U.S. persons engaging in restricted transactions may not, absent a license, use measures other than the security requirements and other applicable conditions to mitigate the risk posed by country-of-concern or covered-person access.

Some commenters provided feedback on the security requirements that would govern restricted transactions. As explained in the ANPRM, CISA will be soliciting comments on the proposed security requirements as part of a separate notice-and-comment process in parallel with this NPRM, and the Department urges commenters to provide any comments on the security requirements through that process.

2. Section 202.258—Vendor Agreement

The proposed rule defines a ''vendor agreement'' as 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. The ANPRM contemplated defining the term ''cloud-computing services'' as that term is defined in NIST Special Publication (''SP'') 800–145.[68] NIST SP 800–145 describes cloud computing in a way that includes different essential characteristics, deployment models, and service models, such as ''Infrastructure as a Service (IaaS),'' ''Platform as a Service (PaaS),'' and ''Software as a Service (SaaS).''[69] Because cloud computing is just one example of several types of services that may be involved in a vendor agreement, it does not appear useful to separately or specially define that term in the proposed rule at this time. The Department may consider issuing guidance in the future that describes cloud computing in reference to the NIST definition.

3. Section 202.217—Employment Agreement

The proposed rule defines an ''employment agreement'' as 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.

4. Section 202.228—Investment Agreement

The proposed rule defines an ''investment agreement'' as any 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. The proposed rule categorically excludes certain passive investments that do not pose an unacceptable risk to national security because they do not give countries of concern or covered persons a controlling ownership interest, rights in substantive decision-making, or influence through a non-controlling interest that could be exploited to access government-related data or bulk U.S. sensitive personal data. Specifically, the proposed rule excludes from ''investment agreement'' investments (1) in any publicly traded security, in any security offered by any investment company that is registered with the United States Securities and Exchange Commission, such as index funds, mutual funds, exchange-traded funds, or made as limited partners (or equivalent) into a venture capital fund, private equity fund, fund of funds, or other pooled investment fund, if the limited partner's contributions and influence are circumscribed as set forth in the proposed rule; (2) that give the covered person less than 10 percent of total voting and equity interest in a U.S. person; and (3) that do not give a covered person rights beyond those reasonably considered to be standard minority shareholder protections.

With respect to the requirement of a de minimis percentage of total voting and equity interest, the Department is considering a range of different proposals. The proposed rule's definition of ''investment agreement'' would apply to investments that give a covered person a certain percentage or more of total voting and equity interest in a U.S. person, even where that investment is not accompanied by other

[68] 89 FR 15788.

[69] *See* Peter Mell & Timothy Grance, *The NIST Definition of Cloud Computing* (NIST, SP 800–145, Sept. 2011), *https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf* [*https://perma.cc/HUJ5-B2JS*].

formal rights beyond standard minority shareholder protections. The proposed rule would include this de minimis threshold to account for the unacceptable national security risk posed by otherwise passive investments that may provide investors with meaningful economic leverage or informal influence over access to a company's assets (like sensitive personal data) even when the investors do not obtain formal rights, control, or access beyond standard minority shareholder protections. The proposed rule would tentatively set this threshold number at 10 percent to exclude truly passive investments while also capturing investments that informally may provide covered persons with influence that presents unacceptable national security risks. The Department is also considering de minimis thresholds that are significantly lower and higher than this percentage, such as the 5 percent threshold above which investors must publicly report their direct or indirect beneficial ownership of certain covered securities under the Securities Exchange Act of 1934, 15 U.S.C. 78m(d). As a result, the final figure in the proposed rule could potentially cover passive investments that provide less (or more) than 10-percent voting and equity interests in a U.S. person. The Department invites public comment on the specific de minimis threshold that should be used in this exception for passive investments.

C. Subpart E—Exempt Transactions

As previewed in the ANPRM, the proposed rule exempts several classes of data transactions from the scope of the proposed rule's prohibitions.

1. Section 202.501—Personal Communications; Section 202.502—Information or Informational Materials; and Section 402.503—Travel

The proposed rule exempts three classes of data transactions to the extent that they involve data that is statutorily exempt from regulation under IEEPA: personal communications, information or informational materials, and data that is ordinarily incident to travel to or from another country.

One comment suggested clarifying that the exemption for personal communications that do ''not involve a transfer of anything of value'' under 50 U.S.C. 1702(b)(1) is ''inclusive of business and commercial transactions.'' The proposed rule makes no change in response to this comment, as the clarification does not seem necessary at this time, given the scope of the statutory exemption and the proposed rule. Section 1702(b)(1) applies to any ''personal communication,'' so it would be inappropriate to rely on that statutory language to exempt, as this comment suggests, ''business and commercial transactions.'' Further, the categories of sensitive personal data encompassed by the proposed rule do not include any personal communications. For example, fingerprints and other biometric identifiers, human genetic testing results, and data about financial assets and liabilities are not ''communications'' from one person to another. Any clarification of the phrase ''a transfer of anything of value,'' therefore, does not appear necessary. To the extent the commenters, a group of trade associations representing telecommunications providers, are concerned that personal communications between individuals that do not involve a transfer of anything of value are business transactions from their perspective, as purveyors of telecommunications services, the Department refers the commenters to the qualified exemption for telecommunications services in proposed § 202.509.

The Department discusses the exemption for information or informational materials in part VI of this preamble.

Although not raised by commenters, the proposed rule also adds a separate exemption for data transactions that are ordinarily incident to travel to or from another country, such as arranging travel or importing baggage for personal use. This exemption implements and tracks the statutory exemption in 50 U.S.C. 1702(b)(4).

2. Section 202.504—Official Business of the United States Government

Adopting the approach contemplated in the ANPRM without change, the proposed rule exempts data transactions to the extent that they are for (1) the conduct of the official business of the United States Government by its employees, grantees, or contractors; (2) 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 (3) transactions conducted pursuant to a grant, contract, or other agreement entered into with the United States Government. Most notably, this exemption would exempt grantees and contractors of Federal departments and agencies, including the Department of Health and Human Services, the Department of Veterans Affairs, the National Science Foundation, and the Department of Defense, so that those agencies can pursue grant-based and contract-based conditions to address risks that countries of concern can access sensitive personal data in transactions related to their agencies' own grants and contracts, as laid out in section 3(b) of the Order—without subjecting those grantees and contractors to dual regulation.

3. Section 202.505—Financial Services

Section 2(a)(v) of the Order exempts any transaction that is ''ordinarily incident to and part of the provision of financial services, including banking, capital markets, and financial insurance services, or required for compliance with any Federal statutory or regulatory requirements, including any regulations, guidance, or orders implementing those requirements.'' [70] The proposed rule defines these exempt transactions in further detail. Notably, the proposed rule exempts 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, while still prohibiting these marketplaces from conducting data transactions that involve data brokerage), as well as exempting the transfer of personal financial data or covered personal identifiers for the provision or processing of payments or funds transfers.

Numerous commenters expressed support for the financial-services exemption. Commenters expressed appreciation for the exemption's careful scoping to enable business and commercial transactions. Commenters sought specific edits to the payment-processing part of the exemption to ensure that it covers operations involving payment dispute resolution, payor authentication, tokenization, payment gateway, payment fraud detection, payment resiliency, mitigation and prevention, and payment-related loyalty point program administration. The Department appreciates these suggested clarifications, and the proposed rule incorporates these proposed edits by explicitly adding the provision of services ancillary to processing payments and funds transfers, with the suggested examples, to the list of exempt financial services transactions.[71] The financial-services exemption aims to identify the low-risk business and

[70] 89 FR 15423.

[71] 89 FR 15794.

commercial transactions that should continue unimpeded while also ensuring that the Order and its implementing regulations do not serve as a broader economic decoupling from countries of concern. These edits are consistent with that purpose.

Another commenter also suggested that investment-management services be included in the financial-services exemption. The Department does not intend to impede activities that are ordinarily incident to and part of 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 executing trades within a securities portfolio based upon instructions from an investment advisor). For further clarity, the proposed rule explicitly adds investment-management services to the financial-services exemption set out in §§ 202.505(a)(1) and 202.505(a)(6).

One commenter requested an exemption for cargo-related information containing listed identifiers. The Department believes this comment is focused on scenarios in which bulk personal identifiers are transferred as part of shipping purchased goods internationally. The Department declines to adopt a separate exemption, or an expansion of the scope of the exemption for transfers of data required by or authorized by Federal law or international agreement, for cargo-related information because the proposed rule already exempts the transfer of personal financial data or covered personal identifiers incidental to the purchase and sale of goods and services. This existing exemption appears to adequately address the scenario raised by the commenter. Thus, the proposed rule adopts the approach described in the ANPRM.

Although not raised by any commenters, the Department is also considering whether and how the financial-services exemption should apply to employment and vendor agreements between U.S. financial-services firms and covered persons where the underlying financial services provided do not involve a country of concern. Under this exemption, U.S. persons would be required to evaluate whether a particular data transaction (such as a transaction involving data brokerage or a vendor, employment, or investment agreement) is ''ordinarily incident to and part of'' the provision of financial services such that it is treated as an exempt transaction.[72] At one end of the spectrum, and as previewed by Example 53 in the ANPRM, if a U.S. financial institution or financial-services company uses a data center operated by a covered person in a country of concern to facilitate payments to U.S. persons in that country of concern, the proposed rule would treat that vendor agreement as ''ordinarily incident to and part of'' the facilitation of those payments—and thus exempt.[73] *See* § 202.505(b)(3). On the other end of the spectrum, and as previewed by Example 27 in the ANPRM, if a U.S. financial institution or financial-services company hires a covered person as a data scientist with access to its U.S. customers' bulk personal financial data to develop a new app that could be sold as a standalone product to the company's customers, the proposed rule would treat this employment agreement as not ''ordinarily incident to and part of'' the financial services provided by the U.S. company—and thus not exempt.[74] *See* § 202.217(b)(4).

Between those two ends of the spectrum, the Department is considering whether the transactions in the following new examples should be treated as exempt transactions or as restricted transactions:

- *New example in § 202.505(b)(4).* Same as Example 3 (*see* § 202.505(b)(3)), but the underlying payments are between U.S. persons in the United States and do not involve a country of concern: A U.S. bank or other financial institution, to facilitate payments that do not involve a covered person or country of concern (*e.g.,* between U.S. persons in the United States), stores and processes the customers' bulk financial data using a data center operated by a third-party service provider in a country of concern, which is a covered person. Should the vendor agreement with the covered person, which is otherwise a restricted transaction, be treated as ''ordinarily incident to and part of'' the U.S. financial institution's facilitation of payments that do not involve a covered person or country of concern?
- *New example in § 202.505(b)(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 access the bulk personal financial data. Should the employment agreement with the covered person as a board director, which is otherwise a restricted transaction, be treated as ''ordinarily incident to and part of'' the U.S. company's provision of wealth-management services to its U.S. clients?

The Department is tentatively considering treating the transactions in both examples as restricted transactions because it does not believe that an employment agreement (including the hiring of board members) or a vendor agreement that gives a covered person access to U.S. persons' bulk sensitive personal data is a reasonable and typical practice in providing the underlying financial services that do not otherwise involve covered persons or a country of concern. These transactions therefore appear to pose the same unacceptable national security risk regardless of the kinds of underlying services provided by the U.S. person. The Department welcomes public comment to inform its resolution of this issue, including the extent to which it is reasonable, necessary, and typical practice for U.S. financial-services firms to hire covered persons as employees or vendors with access to U.S. persons' bulk sensitive personal data as part of providing financial services that do not involve a country of concern; why U.S. financial-services firms hire covered persons instead of non-covered persons in those circumstances; and any additional compliance costs that would be incurred if the transactions in these examples were treated as restricted transactions. In addition, after issuance of the final rule, the Department intends to consult the Department of the Treasury and Federal financial regulatory agencies as part of issuing any guidance or advisory opinions regarding the application of the financial-services exemption.

4. Section 202.506—Corporate Group Transactions

As previewed in the ANPRM, the proposed rule exempts covered data transactions to the extent that they are (1) between a U.S. person and its

[72] *Cf., e.g.,* 31 CFR 560.405(c) (discussing OFAC exemption for transactions ''ordinarily incident to a licensed transaction'' as applied to scenarios involving the provision of transportation services to or from Iran), 515.533 n.1 (discussing OFAC exemption for transactions ''ordinarily incident to'' a licensed transaction as applied to scenarios involving the licensed export of items to any person in Cuba); Letter from R. Richard Newcomb, Director, U.S. Dep't of Treas., Off. of Foreign Assets Control, *Re: Iran: Travel Exemption* (Nov. 25, 2003), *https://ofac.treasury.gov/media/7926/download?inline* [*https://perma.cc/3VRL-X886*] (discussing the OFAC exemption for transactions ''ordinarily incident to'' travel as applied to scenarios involving the use of airline-service providers from a sanctioned jurisdiction).

[73] 89 FR 15794.

[74] 89 FR 15789.

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 (such as sharing employees' covered personal identifiers for human-resources purposes; payroll transactions like the payment of salaries and pensions to overseas employees or contractors; paying business taxes or fees; purchasing business permits or licenses; sharing data with auditors and law firms for regulatory compliance; and risk management). The ANPRM called this exemption ''intra-entity transactions.'' [75] For greater clarity and accuracy, the proposed rule revises the name of this exemption to ''corporate group transactions.''

Some commenters requested that the Department broaden the corporate group transactions exemption to include routine business activities performed by third-party service providers. Similarly, commenters proposed augmenting the same exemption to include suppliers and other third-party vendors who are contractually bound to maintain privacy requirements and who engage in product and services development, research, and improvement activities for U.S. companies. The Department declines to incorporate these suggestions because they would not adequately mitigate the threats posed by access to government-related data or bulk U.S. sensitive personal data by a country of concern or covered person. Thus, the proposed rule adopts the approach described in the ANPRM without change, permitting restricted transactions involving vendor agreements to proceed as long as they comply with the proposed rule's security requirements designed to mitigate access to the sensitive personal data by countries of concern and covered persons.

One commenter requested clarification that it would not be a prohibited transaction for a U.S. company to provide access to a global company staff directory to its business office and employees located in a country of concern. Consistent with the approach contemplated in the ANPRM, this scenario would not be a prohibited or restricted transaction under the proposed rule for two independent reasons. First, a company directory containing only contact or demographic data linked to other contact or demographic data would not fall within the definition of ''covered personal identifiers'' and thus would not constitute government-related data or bulk U.S. sensitive personal data. As a result, there would be no covered data transaction in providing such a directory. Second, the U.S. company's sharing of the directory would not be a prohibited or restricted transaction, regardless of whether the business office is a foreign branch or a subsidiary or affiliate: if the business office in the country of concern is a branch of the U.S. company, the branch is part of the same ''U.S. person'' as the U.S. company, and the U.S. company has not engaged in any transaction with a foreign person in the first place. If, by contrast, the business office is a subsidiary or affiliate of the U.S. company, the sharing is an exempt corporate group transaction because a transaction within a corporate group granting its employees access to a company directory is ordinarily incident to ancillary or administrative business operations. (In different circumstances where that exemption is not applicable, a transaction within a corporate group that gives an employee who is a covered person access to government-related data or bulk U.S. sensitive personal data would generally be a restricted employment agreement.)

5. Section 202.507—Transactions Required or Authorized by Federal Law or International Agreements, or Necessary for Compliance With Federal Law

As previewed in the ANPRM, the proposed rule exempts covered data transactions to the extent that they are required or authorized by Federal law, international agreements or specified global health and pandemic preparedness measures, or necessary for compliance with Federal law.

Some commenters requested clarity about whether the exemption for regulatory compliance (which the ANPRM contemplated as part of the financial-services exemption) applies to compliance with all Federal law, not just financial laws.[76] The Department acknowledges that this is a correct understanding of this exemption. To improve clarity and reflect this understanding, the proposed rule moves the exemption for compliance with Federal law from the financial-services exemption to a standalone subpart of the exemption for transactions required or authorized by Federal law or international agreements.

The proposed rule clarifies that, with respect to international agreements authorizing or requiring data transactions, the exemption applies only to international agreements to which the United States is a party. Some commenters requested a non-exhaustive list of international agreements to which this exemption applies. The proposed rule adds an illustrative list of specific international agreements to which this exemption applies.

One commenter sought clarification on whether transactions required or authorized by international agreements include transactions in accordance with arrangements that facilitate international commercial data flows, such as the Global Cross-Border Privacy Rules (''G–CBPR'') and Global Privacy Recognition for Processors (''G–PRP'') Systems of the Global Cross-Border Privacy Rules Forum (''Global CBPR Forum'') and the Asia-Pacific Economic Cooperation (''APEC'') Cross-Border Privacy Rules (''APEC CBPR'') and APEC Privacy Recognition for Processors Systems. These arrangements are outside the scope of the exemption for international agreements. These arrangements consist of frameworks for coordinating national regulatory measures, and they do not facilitate the sharing of data between the U.S. and a country of concern. Thus, data transactions covered by this proposed rule would not be ''pursuant to these arrangements as necessary to meet the definitional requirements of the exemption. The Department further declines to expand the scope of the exemption to incorporate these arrangements, which are designed to address general privacy concerns and other issues rather than the national security risks detailed in the Order. The same commenter also sought clarity as to whether the EU–U.S. Data Privacy Framework (''DPF'') would be such an international agreement. The EU–U.S. DPF is similarly an arrangement that falls outside the scope of the exemption. The EU–U.S. DPF fulfills different objectives than the proposed rule and does not facilitate the sharing of information between a U.S. person and a country of concern or covered person. For example, under the EU–U.S. DPF and pursuant to Executive Order 14086 of October 7, 2022 (Enhancing Safeguards for United States Signals Intelligence Activities), the Attorney General determined that the laws of EU/European Economic Area countries require appropriate safeguards for signals intelligence activities affecting U.S. persons' personal data.[77]

[75] 89 FR 15794.

[76] 89 FR 15794–95.

[77] E. O. 14086, 87 FR 62283 (Oct. 7, 2022); Dep't of Just., Attorney General Designations of the European Union, Iceland, Liechtenstein, and Norway as ''Qualifying States'', 88 FR 44844 (July 13, 2023).

Furthermore, while DPF- and APEC CBPR-certified companies are subject to domestic law, including the Order, no DPF or APEC CBPR countries or jurisdictions are currently designated as countries of concern under this Executive Order. As such, the provisions of the Order would not apply to transfers conducted in reliance on the DPF or APEC CBPR, and any data transactions that the proposed rule does cover would not be ''pursuant to'' such arrangements as required for this exemption. Therefore, the proposed rule adopts the approach contemplated by the ANPRM without change.

6. Section 202.508—Investment Agreements Subject to a CFIUS Action

Adopting the approach contemplated by the ANPRM, the proposed rule exempts investment agreements to the extent that they are the subject of a ''CFIUS action'' as defined in section 202.207 (*i.e.,* CFIUS has suspended a proposed or pending transaction, or entered into or imposed mitigation measures to address a national security risk involving access to sensitive personal data by countries of concern or covered persons). The rationale for this approach is discussed separately in part IV.K of this preamble.

7. Section 202.509—Telecommunications Services

The proposed rule exempts transactions that are ordinarily incident to and part of telecommunications services.

Multiple commenters requested that the proposed rule include an additional exemption for data that is incidental to the provision and delivery of communications services. They asked that this kind of data be carved out from the scope of any restrictions on sensitive personal data for consumers, enterprises, and governments, including but not limited to international calling, mobile voice, and data roaming. Commenters also requested that communications service providers be able to use, disclose, or permit access to covered data obtained from their customers, either directly or indirectly through agents, to initiate, render, bill, and collect for communications services. These commenters assert that global commerce relies on effective and efficient global communications, that restrictions on such bulk U.S. sensitive personal data could hinder the ability of Americans to communicate globally, and that the United States Government has long held a policy of ensuring that communications are enabled even with countries subject to U.S. sanctions.

The Department appreciates the need to ensure Americans' ability to communicate globally, including with and in countries of concern, and does not intend for these regulations to impede the ability of U.S. telecommunications service providers to operate. Accordingly, the Department has included in the proposed rule an exemption that seeks to address this concern. The proposed exemption is intended to be narrowly tailored to ensure that U.S. telecommunications service providers retain the ability to operate unimpeded while also continuing to mitigate the national security risk associated with data brokerage (*i.e.,* the sale of or leasing of access to customer data) to countries of concern and covered persons.

8. Section 202.510—Drug, Biological Product, and Medical Device Authorizations

Under the proposed rule, certain data transactions necessary to obtain and maintain regulatory approval to market a drug, biological product, medical device, or combination product in a country of concern would be exempt from the prohibitions in the proposed rule. This exemption balances the need to mitigate the risks to U.S. national security from the unrestricted transfer of bulk U.S. sensitive personal data to countries of concern against the scientific, humanitarian, and economic interests in enabling the sale of medicines in those countries. The proposed rule includes reporting requirements that will allow the Department to maintain visibility on the type and amount of data that is being transmitted to countries of concern under this exemption.

This exemption is limited to data that is de-identified; required by a regulatory entity to obtain or maintain authorization or approval to research or market a drug, biological product, device, or combination product (*i.e.,* covered product); and reasonably necessary to evaluate the safety and effectiveness of the covered product. For example, de-identified data that is gathered in the course of a clinical investigation and would typically be required for Food and Drug Administration (''FDA'') approval of a covered product would generally fall within the exemption. Conversely, clinical participants' precise geolocation data, even if required by a country of concern's regulations, would fall outside the scope of the exemption because such data is not reasonably necessary to evaluate safety or effectiveness.

The Department recognizes that data collection and submission continue beyond the initial regulatory approval process, and it intends the term ''regulatory approval data'' to include data from post-market clinical investigations (conducted under applicable FDA regulations, including 21 CFR parts 50 and 56), clinical care data, and post-marketing surveillance, including data on adverse events.[78] For example, where continued approval to market a drug in a country of concern is contingent on submission of data from ongoing product vigilance or other post-market requirements, the exemption applies.

The exemption applies even where FDA authorization for a product has not been sought or obtained. The Department does not, in these regulations, intend to require U.S. companies to first seek authorization to market a product in the United States before seeking regulatory approval from a country of concern.

The exemption is limited to transactions that are necessary to obtain or maintain regulatory approval in the country of concern. The Department specifically invites comments on the types of transactions that are necessary to that end. By way of illustration, Example 3 of § 202.510, as proposed, would not exempt a vendor or employment agreement with a covered person to prepare data for submission to a country of concern's regulatory entity because the Department does not currently believe that such transactions are necessary to obtain regulatory approval. The Department seeks comments on whether, and why, such a vendor or employment agreement with a covered person to prepare data for submission is necessary and should be exempt.

As Example 3 reflects, the Department does not currently believe that it is reasonably necessary to use a covered person—as opposed to services provided by the U.S. company itself or by a non-covered person—to prepare data for regulatory submission. Although the marginal risk to national security from granting additional covered persons access to the submission data may be low, given that the submission data is ultimately being transferred directly to the government of

[78] *See* U.S. Food & Drug Admin., *What Is a Serious Adverse Event?* (May 18, 2023), *https://www.fda.gov/safety/reporting-serious-problems-fda/what-serious-adverse-event#:~:text=An%20adverse%20event%20is%20any,medical%20product%20in%20a%20patient* [*https://perma.cc/9Q23-HRWY*] (''An adverse event is any undesirable experience associated with the use of a medical product in a patient'').

a country of concern, the Department believes that a third-party vendor in this scenario may require access to a broader set of data than the regulatory body itself. At the same time, the Department recognizes that regulatory and legal expertise relevant to a country of concern is likely to be concentrated in the country of concern. Employment and vendor transactions in this context would be restricted, not prohibited, transactions, and generally could proceed if the requirements applicable to restricted transactions were followed. The Department welcomes comments that address this scenario and other similar transactions, including the potential impacts to clinical research, medical product development and authorizations, and companies' business practices and operations, as well as the feasibility of obtaining regulatory approval without engaging covered persons to access bulk U.S. sensitive personal data or if such engagements are subject to the security, recordkeeping, and reporting requirements applicable to restricted transactions.

The exemption requires that parties engaged in transactions involving regulatory approval data with countries of concern nonetheless comply with the recordkeeping and reporting requirements otherwise applicable to U.S. persons engaged in restricted transactions, because of the heightened national security risk that arises from transmitting U.S. sensitive personal data or government-related data directly to a government entity in a country of concern.

The Department seeks comment on the proposed scope of this exemption, including on the definition of regulatory approval data and the extent to which data submissions to regulatory entities in countries of concern may involve personally identifiable data.

9. Section 202.511—Other Clinical Investigations and Post-Marketing Surveillance Data

A few commenters expressed concerns that the proposed rule's inclusion of aggregated and anonymized data would prohibit companies from launching clinical investigations in countries of concern. Commenters also noted the possibility that overly restrictive prohibitions might harm biopharmaceutical innovation. The Department has considered these comments and agrees that some exemption or accommodation for clinical research may be appropriate. The Department proposed the exemption in § 202.511 for that purpose. To help inform the appropriate contours of the proposed provision, the Department invites additional comments that illustrate the scope of transactions that might be subject to the proposed rule's restrictions and prohibitions and the consequences for clinical research if the proposed prohibitions and restrictions were applied to that context.

The United States has a national security interest in the development, authorization, and availability of medical products, including medical countermeasures to diagnose, treat, or prevent serious or life-threatening diseases or conditions that may be attributable to biological, chemical, radiological, or nuclear agents. The Department seeks to mitigate the national security risk described in the Order without unduly burdening the biomedical innovation that benefits U.S. persons. The Department is considering how to effectively strike that balance and how to scope an exemption for transactions related to or supporting FDA-regulated research to meet that goal.

The Department is considering the scope of a possible exemption along three axes. First, in terms of the types of data that would be within the exemption; second, in terms of the types of transactions involving that data that would be exempted; and third, in terms of the duration of any exemption.

On the first axis, the Department anticipates that any exemption would concern data obtained in the course of clinical investigations related to drugs, biological products, devices, and combination products, as those terms are defined in the Federal Food, Drug, and Cosmetic Act (''FD&C Act'') and FDA regulations. The Department believes that these products raise the most significant countervailing economic, health, and scientific concerns that might outweigh the national security interests otherwise at stake. The Department seeks comment on whether the exemption should exempt clinical investigations data related to other products, such as foods (including dietary supplements) that bear a nutrient content claim or a health claim, food and color additives, and electronic products, as those terms are defined in the FD&C Act.

The Department also recognizes the existing regulatory framework in these contexts and is evaluating whether these provisions adequately reduce the national security risk associated with the transfer of bulk U.S. sensitive personal data to a country of concern or covered person. The FD&C Act and FDA regulations provide a robust framework to protect the confidentiality and privacy of data collected from subjects in clinical investigations. This current framework of statutory and regulatory requirements protects the rights and safety of human subjects, ensuring that their private information is handled securely. For example, section 505(i) (21 U.S.C. 355(i)) and section 520(g) (21 U.S.C. 360j(g)) of the FD&C Act address the use of investigational new drugs and investigational devices, respectively, in clinical investigations and require that informed consent be obtained from subjects, with certain exceptions.

The implementing regulations established by the FDA in 21 CFR parts 50, 56, 312, and 812 include various requirements, including related to informed consent of human subjects and Institutional Review Boards (''IRBs''). For example, 21 CFR part 56 details requirements for IRB review, approval, and ethical oversight of FDA-regulated clinical investigations. Information about the confidentiality of records must be given to prospective subjects as part of informed consent (21 CFR 50.25(a)(5)), and to approve research, an IRB must determine that, where appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data (21 CFR 56.111(a)(7)). In addition, FDA regulations in 21 CFR part 11 establish requirements to ensure the authenticity, integrity, and, when appropriate, confidentiality of certain electronic records (21 CFR 11.10, 11.30). The FDA further issued a proposed rule in September 2022 proposing to require that certain information about future secondary use of subjects' information or biospecimens be provided to prospective subjects.[79]

These regulations are principally focused on patient privacy, however, and do not directly address the national security concerns that animate the Order. As the Department has explained elsewhere in this preamble, privacy protections, in general, focus on addressing individual rights and preventing individual harm by protecting individuals' right to control the use of their own data and reducing the potential harm to individuals by minimizing the collection of data on the front end and limiting the permissible uses of that data on the back end. National security measures, by contrast, focus on collective risks and externalities that may result from how individuals and businesses choose to sell and use their data, including in lawful and legitimate ways. But the

[79] Protection of Human Subjects and Institutional Review Boards, 87 FR 58733 (proposed Sept. 28, 2022).

Department is evaluating whether these existing regulations—for example, the requirements for informed consent under 21 CFR part 50—could offer sufficiently robust protection to also mitigate national security concerns.

The exemption would also apply to clinical care data indicating real-world performance or safety of products, or post-marketing surveillance data (including pharmacovigilance and post-marketing safety monitoring), where necessary to support or maintain authorization by the FDA. These submissions to FDA involve deidentified data and the exemption arising under proposed § 202.511(a)(2) would apply only to deidentified data.

On the second axis, the Department is considering what kinds of transactions to exempt when they involve data that implicates the exemption—such as, hypothetically, bulk U.S. sensitive personal data collected in the course of an FDA-regulated clinical investigation to develop a drug. One possibility would be to exempt all transactions that are part of the conduct of the investigation. Another possibility would be to limit an exemption to only certain types of transactions that are especially important to the conduct of a clinical investigation and that cannot feasibly be avoided without jeopardizing the clinical investigation.

The Department does not intend to categorically preclude clinical investigations from being conducted in a country of concern and does not believe that the proposed rule, even without a clinical investigation-focused exemption, does so. The proposed rule generally does not prohibit or restrict the flow of data from a country of concern to the United States and does not apply to data unrelated to U.S. persons. The Department seeks additional comments on whether, why, and to what extent it would be necessary for U.S. persons to transmit bulk U.S. sensitive personal data to a covered person in order to support a clinical investigation taking place in a country of concern.

For example, the Department has considered the following hypothetical:

- A U.S. sponsor conducts a clinical investigation to determine the safety and effectiveness of an investigational drug product. The clinical investigation involves a multinational trial with both U.S. citizens and non-U.S. citizens enrolled in the trial at different sites across the world, including in a country of concern, to support authorization of the product in the intended use populations. As part of the investigation, and pursuant to an employment or vendor agreement, the sponsor transmits bulk U.S. sensitive personal data to covered persons in the country of concern to conduct a data analysis of the product's safety and effectiveness across different population groups. This clinical investigation supports an application for a marketing permit for a product regulated by the FDA (*i.e.,* a drug for human use). The trial in this example is subject to the FDA's regulatory framework for clinical investigations.

The Department believes that, absent an exemption, the employment or vendor agreement described in this hypothetical would be a restricted transaction (or a prohibited transaction, if it involves the transfer of bulk human genomic data or biospecimens from which such data could be derived). The Department seeks comments on whether such a vendor agreement should be considered to be ''ordinarily incident to and part of'' a clinical investigation; how prevalent and important the practice of sending bulk U.S. sensitive personal data to a covered person in a country of concern is; and the potential impacts to clinical research, medical product development and authorization, and industry if such transactions were restricted or prohibited.

The Department also seeks comments on how these concerns apply in post-marketing scenarios, such as pharmacovigilance and post-marketing safety monitoring necessary to support or maintain authorization. For example, the Department has considered the following hypothetical:

- A U.S. pharmaceutical company is required to submit reports to the FDA of adverse events related to its FDA-approved drug for human use, consistent with the requirements under 21 CFR 314.80.[80] The firm markets many other drug products; has a wide global distribution, including in a country of concern; and receives thousands of reports per year for its various marketed products. Under a vendor agreement, the firm may outsource processing of these reports to entities outside of the United States, including in a country of concern. The firm may also need to exchange adverse event information about its FDA-approved drug product with its distributors in a country of concern to pool the data and identify any adverse events trends across different population groups or conditions of use and submit those data to the FDA.

As in the context of the clinical investigation, the Department believes that, absent an exemption, the vendor agreements described in this hypothetical would be restricted or prohibited. The Department seeks comments on how pervasive and important the practice of outsourcing the processing of adverse event reports to a covered person is, as well as on how pervasive and important it is to share adverse event information concerning U.S. persons with drug distributors in a country of concern. The Department seeks comments on the potential impacts to patient safety, industry, and the feasibility of obtaining or maintaining regulatory authorizations if such transactions were to be prohibited.

The Department is also aware that, as appropriate and required, certain data related to post-marketing surveillance are made available to global public health authorities, such as the World Health Organization Vigibase. Submissions by the United States Government itself, such as FDA submissions to Vigibase, would be exempt under proposed § 202.504. The Department expects that similar data transactions by U.S. persons, even if such data transactions were considered to be with a country of concern or a covered person so as to fall within the scope of the restrictions and prohibitions, would nonetheless be exempt under proposed § 202.507. The Department seeks specific comments on the nature and type of such submissions and a list of such global health authorities. The Department also notes that, if it is lawfully available to the public from a Federal, State, or local government record or in widely distributed media, such data would not meet the definition of sensitive personal data under § 202.249(b)(2).

FDA regulations include recordkeeping provisions such that FDA investigators can gather information about any data transactions, including to countries of concern. *See* 21 CFR part 312.62. However, in general, FDA's regulations related to clinical investigations do not require sponsors to report data transactions to the FDA in the manner proposed in the recordkeeping and reporting requirements set forth in §§ 202.1101(a) and 202.1102. The Department is considering requiring reporting even for transactions within any exemption to better evaluate the national security risks going forward and seeks comments on the cost and feasibility for industry of also complying with the recordkeeping and reporting requirements set forth in §§ 202.1101(a) and 202.1102 with respect to

[80] An adverse event report describes the experience of an individual who has experienced an adverse event associated with the use of a drug.

transactions related to clinical investigations.

The Department recognizes that U.S. companies employing covered persons—such as foreign persons primarily resident in a country of concern to support a clinical investigation there—may have to adjust data access policies or protocols to limit covered persons' access to bulk U.S. sensitive personal data. The Department seeks comment on this issue, including the costs and feasibility of adopting such policies or protocols and the likely effect of such policies on medical product research and development, as well as obtaining or maintaining regulatory authorization.

The Department also notes that, under § 202.504, covered data transactions that occur as part of federally funded research would be exempt from the proposed rule's prohibitions (although possibly subject to separate restrictions applicable to a Federal grantee, to include requirements established pursuant to section 3(b)(i) of the Order). The Department invites comment on the proportion of pharmaceutical research that would not be exempt under that exemption, the cost and feasibility of complying with different regulatory requirements depending on the source of funding, and the impact on medical product research and development.

If the Department were to implement an exemption for clinical investigations, clinical data, and post-marketing surveillance as described in this section, it could potentially do so through one or more general licenses as opposed to including the exemption in the final rule. General licenses may be a more flexible regulatory tool that can be adjusted to varying circumstances. Preliminarily, however, the Department believes that a codified exemption would provide more clarity and certainty for relevant entities. The Department also invites comments on the best mechanism to implement an exemption for such data transactions.

Finally, on the third axis, the Department is considering whether any exemption, or parts of it, could feasibly be time-limited to allow industry to shift existing processes and operations out of countries of concern over a transition period. The Department is cognizant of the long planning times and high costs associated with clinical research. If the Department does not broadly exempt clinical research from the scope of the prohibitions, it may consider delaying the effective date of the proposed rule with respect to such research to enable affected entities to complete ongoing or imminent trials without disruption or delay, while transitioning planning and policies for future trials. The Department could potentially implement such a delay by general or specific licenses, and could use a set period of time or could limit the exemption to studies already past a certain stage, such as submission of an Investigational New Drug application to the FDA by a set date. The Department seeks comment—taking into account other exemptions, such as for federally funded research—on the number of clinical investigations that would be disrupted, and the extent of such disruption, if the prohibitions were immediately applicable; how long and how to structure any delay to minimize disruption without inviting misplaced reliance; and the best mechanism for implementing such a delay.

10. Other Exemptions

The Department is considering whether it is necessary or appropriate to adopt a tailored exemption that would permit covered data transactions involving the export to countries of concern or transfer or sale to covered persons of certain human biospecimens, like blood plasma, intended for direct medical use that the proposed rule would otherwise prohibit. The Department welcomes views about the specific types of biospecimens exported to countries of concern, or transferred or sold to covered persons for direct medical use that the Department should consider exempting from the prohibition on bulk transfers of human genomic data or biospecimens from which bulk human genomic data could be derived. Important considerations could include the importance of the biospecimens for direct medical use; the relative ease with which a country of concern or covered person could derive bulk human genomic data from the biospecimens; the economic and humanitarian value of permitting such transactions; and any other national security concerns the Department should consider.

A few commenters requested that the Department create a new exemption for data processed by a covered person on behalf of a U.S. person for product research, development, or improvement where the U.S. person directs the manner of data processing and contractually binds the covered person to maintain the privacy and security of the data. These comments were too vague to be addressed or implemented. For example, they did not identify the kinds of products that the U.S. person would seek to develop or the kinds of data that would be required for that development. In any case, as the Department discusses in part IV.D.1 of this preamble, countries of concern have the legal authority and political systems to force, coerce, and influence entities in their jurisdictions to share their data and access with the government. Entities operating in these jurisdictions may be legally compelled to comply with these requests, regardless of their trustworthiness or contractual commitments. The Department assesses that the kind of contractual provisions contemplated by these commenters would not adequately mitigate the risk that countries of concern could compel these covered persons to provide them access to government-related data or Americans' bulk U.S. sensitive personal data. Further, other commenters expressed concern about relying on private parties to monitor and enforce contractual provisions on their own, as discussed in part IV.A.16 of this preamble.

D. Subpart F—Determination of Countries of Concern

1. Section 202.601—Determination of Countries of Concern

As explained in the ANPRM and above in part II of this preamble, countries of concern could exploit government-related data or bulk U.S. sensitive personal data for a range of activities detrimental to U.S. national security, including coercion, blackmail, surveillance, espionage, malicious cyber-enabled activities, malign foreign influence, curbing political dissent and opposition, and tracking and building profiles on potential targets.

The Order instructs the Attorney General to ''identify, with the concurrence of the Secretary of State and the Secretary of Commerce, countries of concern.'' [81] In the proposed rule, the Attorney General has determined, with the concurrence of the Secretaries of State and Commerce, that the governments of six countries—the People's Republic of China (''China'' or ''PRC''), along with the Special Administrative Region of Hong Kong and the Special Administrative Region of Macau; the Russian Federation (''Russia''); the Islamic Republic of Iran (''Iran''); the Democratic People's Republic of Korea (''North Korea''); the Republic of Cuba (''Cuba''); and the Bolivarian Republic of Venezuela (''Venezuela'')—have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or the security and safety of U.S. persons, and pose a significant risk of exploiting government-related data or bulk U.S.

[81] 89 FR 15424.

sensitive personal data to the detriment of the national security of the United States or the security and safety of U.S. persons.

In determining that a country has engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or the security and safety of U.S. persons, the proposed rule accounts for a range of conduct, including transnational repression; malicious cyber activities; sanctions evasion; theft of intellectual property, trade secrets, and technology; foreign malign influence;[82] and human-rights abuses. Even where human-rights abuses do not directly involve U.S. persons, the Department considers human-rights abuses to be significantly adverse to national security because of their indirect effects. For example, by developing, testing, and using sophisticated surveillance technology on their own populations or conducting surveillance on their own populations, countries can expand the use of those methods and potentially deploy them directly against U.S. persons or U.S. interests in the future.[83] Furthermore, a country that commits human-rights violations shows its disregard for international norms and its intention to use the coercive power of the state to accomplish its policy goals. For example, countries that commit human-rights violations may also attempt to surveil or coerce their citizens in the United States, including through transnational repression.[84] Based on its experience, the Department believes that such factors demonstrate that a country presents a risk that, if provided access, it would exploit government-related data or bulk U.S. sensitive personal data to the detriment of the national security of the United States or the security and safety of U.S. persons.

During the ANPRM's comment period, commenters requested that the proposed rule include criteria and a transparent process for the Department of Justice to designate countries of concern, including by conducting robust interagency discussion and soliciting public comment. The proposed rule makes no change in response to this comment. The Order already requires that prior to amending the list of countries of concern, the Department must obtain concurrence by the Secretary of State and the Secretary of Commerce and undertake a rulemaking that is subject to the ordinary process of robust interagency review and notice and public comment. In addition to the opportunity for notice and public comment on this proposed rule's identification of countries of concern, the Department took the optional step of issuing an ANPRM to permit an additional opportunity for public comment on the contemplated countries of concern.

One commenter supported aligning the list of countries of concern with the list established by the Department of Commerce in 15 CFR 791.4, which was adopted pursuant to Executive Order 13873. The ANPRM already contemplated identifying the same countries as countries of concern under the Order as the Department of Commerce identified as foreign adversaries under Executive Order 13873. The proposed rule adopts that approach and identifies those same countries for reasons explained further in this part.

Other commenters expressed concerns that the list of six countries of concern contemplated in the ANPRM is too narrow and does not adequately address entities based in third countries that engage in or facilitate surveillance on U.S. citizens. The proposed rule makes no change in response to this comment. As the ANPRM described, the Department intends to establish this program by issuing proposed rulemakings in tranches based on priority and effective administration of the program. The Department intends to continue working closely with the Department of State, Department of Commerce, and other agencies to monitor the effectiveness of the regulations and the need for any changes. Similarly, one commenter suggested that the Department consider designating a larger group of countries as countries of concern based upon those countries' lack of privacy laws or lack of enforcement of their privacy laws. The Department declines to adopt this approach at this time. The Order's focus is addressing the national security risk posed by country of concern access to government-related data or Americans' bulk U.S. sensitive personal data. The Order does not establish a general data privacy regime. The proposed rule thus maintains the country of concern framework described in the ANPRM without change.

Informed by the ANPRM comments and the Department's independent research and analysis, which are summarized in part IV.D of this preamble, the Department proposes identifying the same countries of concern as those identified by the Department of Commerce in implementing Executive Order 13873. The proposed rule's definition of each of these countries includes political subdivisions, agencies, or instrumentalities of those countries. In addition, the Order specifically defines a ''country of concern,'' and the Department has determined that every country included on the list of countries of concern meets that definition.

The Department seeks comment from the public on the proposed countries of concern. The proposed rule identifies these six countries as countries of concern for the following reasons.

a. China

The Department has determined, with the concurrence of the Secretaries of State and Commerce, that China has engaged in a long-term pattern of conduct significantly adverse to the national security of the United States and the security and safety of U.S. persons. Among other conduct significantly adverse to the national security of the United States and the security and safety of U.S. persons, China engages in transnational repression;[85] steals trade secrets and intellectual property;[86] conducts foreign malign influence;[87] commits human rights abuses that could help it develop the capability to surveil, manipulate, or extort U.S. persons;[88] and conducts extensive malicious cyber activities.[89]

[82] *See* 50 U.S.C. 3059(f)(2).

[83] Nat'l Counterintel. & Sec. Ctr., *China's Collection of Genomic and Other Healthcare Data from America: Risks to Privacy and U.S. Economic and National Security* 3–4 (Feb. 2021), *https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/NCSC_China_Genomics_Fact_Sheet_2021revision20210203.pdf* [*https://perma.cc/BL4H-WJSW*].

[84] Press Release, U.S. Dep't of Just., *Two Arrested for Operating Illegal Overseas Police Station of the Chinese Government* (Apr. 17, 2023), *https://www.justice.gov/opa/pr/two-arrested-operating-illegal-overseas-police-station-chinese-government* [*https://perma.cc/XM9B-2BU7*].

[85] Press Release, U.S. Dep't of Just., *Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians* (Mar. 25, 2024), *https://www.justice.gov/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived* [*https://perma.cc/YQC7-JDCU*].

[86] *Id.;* Off. of the Dir. of Nat'l Intel., *Annual Threat Assessment of the U.S. Intelligence Community,* at 12 (Feb. 5, 2024), *https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf* [*https://perma.cc/FX84-ZR7E*].

[87] Off. of the Dir. of Nat'l Intel., *supra* note 86, at 12.

[88] Nat'l Counterintel. & Sec. Ctr., *supra* note 83, at 3–4.

[89] Off. of the U.S. Trade Rep., *Four-Year Review of Actions Taken in the Section 301 Investigation: China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation,* at 15–33 (May 14, 2024), *https://ustr.gov/sites/default/files/05.14.2024%20Four%*

Continued

According to the Office of the Director of National Intelligence (''ODNI''), China is ''the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks.'' [90] China's cyber espionage operations have included ''compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations.'' [91] China ''conducts cyber intrusions that are targeted to affect U.S. and non-U.S. citizens beyond its borders—including journalists, dissidents, and individuals it views as threats—to counter views it considers critical of [Chinese Communist Party] narratives, policies and actions.'' [92] It also conducts malign influence operations to ''sow doubts about U.S. leadership, undermine democracy, and extend [China's] influence.'' [93]

Because China aggressively obtains and exploits data on U.S. persons through both commercial means and theft, and has growing artificial intelligence capabilities, it poses a significant risk of exploiting government-related data or Americans' bulk U.S. sensitive personal data to the detriment of the national security of the United States and the security and safety of U.S. persons.

China aggressively obtains and exploits data on U.S. persons via commercial and illicit means. The National Counterintelligence and Security Center (''NCSC'') has warned that China ''views bulk personal data, including healthcare and genomic data, as a strategic commodity to be collected and used for its economic and national security priorities.'' [94] As ODNI has also explained, China ''has engaged in extensive and years-long efforts to accumulate structured datasets, in particular on U.S. persons, to support its intelligence and counterintelligence operations,'' [95] and is ''rapidly expanding and improving its artificial intelligence and big data analytics capabilities for intelligence operations.'' [96] China ''uses a number of methods to obtain data.'' [97] For example, China engages in the ''wholesale theft'' of sensitive personal data of U.S. persons.[98] The following are some examples of the PRC's aggressive campaign to steal and exploit government-related data or bulk U.S. sensitive personal data: [99]

- In 2024, a Federal grand jury returned an indictment against hackers working for Chinese intelligence services for, among other things, targeting high-ranking United States Government officials and staffers for a presidential campaign by sending thousands of malicious emails.[100] The hackers potentially compromised the email and cloud storage accounts and telephone records belonging to millions of Americans.[101]
- In 2020, a Federal grand jury returned an indictment against four members of the PRC's People's Liberation Army for hacking U.S. credit-reporting agency Equifax in 2017.[102] The hackers stole the data of approximately 145 million victims, obtaining, ''in a single breach, . . . the sensitive personally identifiable information for nearly half of all American citizens.'' [103]
- In 2015, PRC hackers stole the health records of 78.8 million persons from U.S. health insurance provider Anthem, Inc.,[104] and stole the background investigation records of 21.5 million prospective, current, and former Federal employees and contractors from the Office of Personnel Management.[105]
- In 2021, a Federal grand jury returned an indictment against four Chinese nationals working for PRC intelligence services for hacking into the computer systems of dozens of companies, universities, and government entities between 2011 and 2018 to steal sensitive technical technology and data, including material related to genetic sequencing.[106]
- In 2021, cyber actors linked to China's intelligence services exploited previously undisclosed vulnerabilities in Microsoft Exchange Server, compromising tens of thousands of computers and networks, including those in the United States, in a massive operation.[107]
- In 2018, a Federal grand jury returned an indictment against two PRC intelligence-affiliated officials for conducting a campaign targeting the computer networks and systems of technology and cloud-service companies in at least a dozen U.S. States, as well as United States Government agencies, to access their customers' data.[108] At least eight major

20Year%20Review%20of%20China%20Tech%20Transfer%20Section%20301%20(Final).pdf [*https://perma.cc/W6FN-4C38*].

[90] Off. of the Dir. of Nat'l Intel., *supra* note 86, at 12.

[91] Off. of the Dir. of Nat'l Intel., *Annual Threat Assessment of the U.S. Intelligence Community* 10 (Feb. 6, 2023), *https://www.odni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf* [*https://perma.cc/4B2Y-7NVD*].

[92] *Id.*

[93] *Id.*

[94] Nat'l Counterintel. & Sec. Ctr., *supra* note 83, at 1.

[95] *In Camera, Ex Parte* Classified Decl. of Casey Blackburn, Assistant Dir. of Nat'l Intel., Doc. No. 2066897 at Gov't App. 10 ¶ 31, *TikTok Inc.* v. *Garland,* Case Nos. 24–1113, 24–1130, 24–1183 (D.C. Cir. July 26, 2024) (publicly filed redacted version) (hereinafter ''Blackburn Decl.'').

[96] *Id.* at Gov't App. 10 ¶ 30.

[97] *Id.* at Gov't App. 10 ¶ 32.

[98] *The Strategic Competition Between the U.S. and the Chinese Communist Party: Hearing Before the H. Select Comm.,* 108th Cong. (2024) (statement of Christopher Wray, Director, Fed. Bureau of Investig.), *https://www.fbi.gov/news/speeches/director-wrays-opening-statement-to-the-house-select-committee-on-the-chinese-communist-party* [*https://perma.cc/89CA-DPHQ*]; *see also* Nat'l Intel. Council, *supra* note 5, at 3.

[99] Nat'l Intel. Council, *supra* note 5, at 3; Wray, *supra* note 98.

[100] Press Release, U.S. Dep't of Just., *supra* note 85; Indictment, *United States* v. *Gaobin,* No. 24–cr–43 (E.D.N.Y. filed Jan. 30, 2024).

[101] Indictment ¶ 15, *Gaobin,* 24–cr–43.

[102] Indictment ¶¶ 2–3, *United States* v. *Zhiyong,* No. 20–cr–046 (N.D. Ga. filed Jan. 28, 2020); *see also* Press Release, U.S. Dep't of Just., *Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax* (Feb. 10, 2020), *https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking* [*https://perma.cc/2TW4-2HGP*].

[103] Indictment ¶ 3, *Zhiyong,* No. 20–cr–046; *see also* Nat'l Intel. Council, *supra* note 5, at 4; Christopher Wray, Dir., Fed. Bureau of Investig., The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Sec. of the United States, Address at the Hudson Institute Event on China's Attempt to Influence U.S. Institutions (July 7, 2020), *https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states* [*https://perma.cc/LMJ6-882S*].

[104] Nat'l Counterintel. & Sec. Ctr., *supra* note 83, at 3.

[105] U.S. Off. of Pers. Mgmt., *Cybersecurity Incidents, https://www.opm.gov/cybersecurity-resource-center/#url=Cybersecurity-Incidents* [*https://perma.cc/V87Q-2K6W*]; Nat'l Counterintel. & Sec. Ctr., *supra* note 83.

[106] *See* Press Release, U.S. Dep't of Just., *Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research* (July 19, 2021), *https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion* [*https://perma.cc/KJ76-KRKS*]; Indictment ¶ 4, *United States* v. *Xiaoyang,* No. 21–cr–01622 (S.D. Cal. filed May 28, 2021).

[107] Press Release, The White House, *The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China* (July 19, 2021), *https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/* [*https://perma.cc/5ESU-43VY*].

[108] *See* Press Release, U.S. Dep't of Just., *Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information* (Dec. 20, 2018), *https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion* [*https://perma.cc/5M68-*

managed service providers were compromised, as well as the National Aeronautics and Space Administration and the Department of Energy.[109] Over 12 years, hackers stole hundreds of gigabytes of data, including the personally identifiable information of over 100,000 U.S. Navy personnel.[110]

As ODNI has explained, China ''also tries to leverage access through its relationships with Chinese companies, strategic investments in foreign companies, and by purchasing large data sets.'' [111] China and Chinese companies ''have sought to acquire sensitive health and genomic data on U.S. persons through, for example, investment in U.S. firms that handle such data or by partnering with healthcare or research organizations in the United States to provide genomic sequencing services.'' [112] China also strategically acquires sensitive personal data on U.S. persons through commercial means, such as by investing in U.S. firms through Chinese companies and engaging in partnerships with hospitals, universities, and research organizations.[113] China employs a wide array of means to ensure that the Chinese government benefits from Chinese companies' relationships with U.S. companies. Not only do direct investments by Chinese companies facilitate China's strategic objectives,[114] but those direct investments also promote a strategy of ''military-civil fusion'' that ensures that China's military can ''acquire advanced technologies and expertise developed by [Chinese] companies, universities, and research programs that appear to be civilian entities.'' [115]

These commercial means of obtaining sensitive personal data on U.S. persons are paired with China's national-security laws that compel companies to share data they have collected on U.S. persons with the Chinese government.[116] As the Department has explained, ''China has enacted the world's most comprehensive set of laws, regulations, and national plans to broadly define its national and public security interests in data and to govern data collection, sales, sharing, and storage.'' [117] Given ''the authoritarian structures and laws of the PRC regime, Chinese companies lack meaningful independence from the PRC's agenda and objectives,'' and ''even putatively 'private' companies based in China do not operate with independence from the government and cannot be analogized to private companies in the United States.'' [118] This regime includes ''several laws that, in concert, allow the Chinese government to access sensitive personal data possessed by Chinese companies,'' [119] such as the following:

- The National Security Law of the People's Republic of China (promulgated by the Standing Committee of the National People's Congress, July 1, 2015, effective July 1, 2015), which ''imposes broad obligations on corporations as well as citizens to assist and cooperate with the Chinese government in protecting what it defines as national security'' and to ''assist military agencies and relevant departments with national security efforts.'' [120]
- The Cybersecurity Law of the People's Republic of China (promulgated by the Standing Committee of the National People's Congress, Nov. 7, 2016, effective June 1, 2017), which ''requires Chinese companies to store their data within China, to cooperate with crime and security investigations, and to allow full access to data to Chinese authorities.'' [121]
- The Anti-Terrorism Law of the People's Republic of China (promulgated by the Standing Committee of the National People's Congress, Dec. 27, 2015, effective Jan. 1, 2016, amended Apr. 27, 2018), which authorizes the Chinese government to conduct ''electronic monitoring,'' ''irregular inspections,'' and '''terrorism' investigations and requires individuals and organizations to comply, in secret, with such investigations''; broadly ''defines 'terrorism' as ''propositions and actions that . . . create social panic, endanger public safety, infringe on personal and property rights, or coerce state organs or international organizations to achieve their political, ideological, and other objectives''; and imposes on all organizations and individuals ''the obligation to assist and cooperate with relevant departments in anti-terrorism work.'' [122]
- The Counter-Espionage Law of the People's Republic of China (promulgated by the Standing Committee of the National People's Congress, Nov. 1, 2014, amended Apr. 26, 2023, effective July 1, 2023), which authorizes ''national security agency staff'' to ''enter restricted areas, locations, and units'' and to ''inspect the electronic devices, facilities, and relevant procedures and tools of concerned individuals and organizations,'' and also requires ''citizens and organizations'' to ''support and assist'' such efforts.[123]

These laws all ''contain provisions that prohibit individuals and organizations from revealing when and if the Chinese government has requested any assistance or information from them.'' [124] As a result, China can covertly obtain data on U.S. persons in the possession of Chinese companies without meaningful due process and independent judicial oversight. China's commercial acquisitions of data also contribute to the government's growing repository of data on U.S. persons.[125]

China's access to bulk U.S. sensitive personal data—whether via commercial means or outright theft—fuels its development of artificial intelligence capabilities, which China believes will drive the next revolution in military affairs.[126] The Office of the Director of National Intelligence assesses that China is ''rapidly expanding and improving its

677J]; *see also* Indictment ¶¶ 3–5, *United States* v. *Zhu,* No. 18–cr–891 (S.D.N.Y. filed Dec. 17, 2018).

[109] Indictment ¶¶ 5–6, *Zhu,* No. 18–cr–891.

[110] Indictment ¶ 10, *Zhu,* No. 18–cr–891.

[111] Blackburn Decl., *supra* note 95, at Gov't App. 11 ¶ 33.

[112] *Id.* at Gov't App. 11 ¶ 33(a).

[113] Nat'l Counterintel. & Sec. Ctr., *supra* note 83, at 2.

[114] Off. of the U.S. Trade Representative, Exec. Off. Of the Pres., *Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974* 63 (Mar. 22, 2018), *https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF* [*https://perma.cc/SAS4-JSNK*].

[115] Press Release, U.S. Dep't of Def., *DOD Releases List of People's Republic of China (PRC) Military Companies in Accordance with Section 1260H of the National Defense Authorization Act for Fiscal Year 2021* (Jan. 31, 2024), *https://www.defense.gov/News/Releases/Release/Article/3661985/dod-releases-list-of-peoples-republic-of-china-prc-military-companies-in-accord/* [*https://perma.cc/S7HA-384R*].

[116] Nat'l Counterintel. & Sec. Ctr., *supra* note 83, at 4.

[117] Newman Decl., *supra* note 40, at Gov't App. 49 ¶ 16.

[118] *Id.* at Gov't App. 49 ¶ 17.

[119] *Id.* at Gov't App. 19 ¶ 18.

[120] *Id.* at Gov't App. 49–50 ¶ 19; *see* Exh. A to Newman Decl., *supra* note 40.

[121] Newman Decl., *supra* note 40, at Gov't App. 50–51 ¶ 20; *see* Exh. B to Newman Decl., *supra* note 40.

[122] Newman Decl., *supra* note 40, at Gov't App. 51 ¶ 21; *see* Exh. C. to Newman Decl., *supra* note 40.

[123] Newman Decl., *supra* note 40, at Gov't App. 51–52 ¶ 23; *see* Exh. E to Newman Dec., *supra* note 40.

[124] Newman Decl., *supra* note 40, at Gov't App. 52 ¶ 24.

[125] Lisa Monaco, Deputy Att'y Gen., U.S. Dep't of Just., Remarks on Disruptive Technologies at Chatham House (Feb. 16, 2023), *https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-disruptive-technologies-chatham* [*https://perma.cc/NW6D-HM6Q*] (''So if a company operating in China collects your data, it is a good bet that the Chinese government is accessing it.'').

[126] Elsa B. Kania, ''*AI Weapons*'' *in China's Military Innovation,* Brookings Inst. (Apr. 2020), *https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_ai_weapons_kania_v2.pdf* [*https://perma.cc/JPM7-YHV5*].

AI and big data analytics capabilities for intelligence operations'' [127] and ''increasing [its] ability to analyze and manipulate large quantities of personal information in ways that will allow [it] to more effectively target and influence, or coerce, individuals and groups in the United States.'' [128] In turn, China's advances in artificial intelligence ''deepen[] the threats posed by cyberattacks and disinformation campaigns'' that China is using ''to infiltrate [U.S.] society, steal [U.S.] data and interfere in [U.S.] democracy.'' [129]

b. Cuba

The Department has determined, with the concurrence of the Secretaries of State and Commerce, that Cuba has engaged in a long-term pattern of conduct significantly adverse to the national security of the United States and the security and safety of U.S. persons. The United States has long recognized that the Cuban government presents a national security threat to the United States. Among other conduct significantly adverse to the national security of the United States and the security and safety of U.S. persons, Cuba conducts intelligence operations against the United States; commits human-rights abuses that, among other effects, contribute to a significant increase in migration into the United States and its neighbors; [130] and sponsors terrorism.[131] Because of the Cuban government's actions, the United States has imposed some form of economic sanctions on Cuba since the early 1960s, including under the Trading with the Enemy Act of 1917. The United States currently maintains a comprehensive economic embargo on Cuba.[132]

Because Cuba has engaged in long-standing efforts to target the United States Government and United States Government personnel for intelligence purposes, Cuba poses a significant risk of exploiting government-related data or Americans' bulk U.S. sensitive personal data to the detriment of the national security of the United States and the security and safety of U.S. persons. According to ODNI, Cuba's intelligence capabilities pose a ''significant threat[ ]'' to the United States.[133] For decades, Cuban intelligence services have sought to obtain information about the United States Government and to target U.S. persons to pursue Cuba's interests, including espionage. For example, in 2024, a former U.S. Department of State employee who served as U.S. Ambassador to Bolivia admitted to secretly acting as an agent of Cuba for decades and received a 15-year prison sentence.[134] In another example, in 2010, a U.S. Department of State official and his wife were sentenced to lengthy prison sentences for participating in a ''nearly 30-year conspiracy to provide highly classified U.S. national defense information'' to Cuba.[135] In 2004, a Federal grand jury returned an indictment against an individual for conspiring to share information related to U.S. national defense with Cuba, including helping Cuban intelligence services ''spot, assess, and recruit U.S. citizens who occupied sensitive national security positions or had the potential of occupying such positions in the future to serve as Cuban agents.'' [136] In 2002, an employee at the Defense Intelligence Agency was sentenced to 25 years in prison for spying on behalf of Cuba, including sharing the identities of American undercover intelligence officers working in Cuba with the Cuban government.[137] In 2022, Team Telecom recommended that the Federal Communications Commission (''FCC'') deny an application for a license for a subsea telecommunications cable that would have directly connected the United States to Cuba.[138] Team Telecom highlighted Cuba's history of espionage and intelligence activities targeting the United States.[139] Because Cuba's state-owned telecommunications monopoly would control the cable, Team Telecom concluded that the cable would give the Cuban government the ability and opportunity to access U.S. persons' internet traffic, data, and communications transiting the cable, and make the Cuban government an even greater counterintelligence threat to the United States.[140]

Cuba also has strong ties to both China and Russia and might share any information it obtains on U.S. persons with either of those countries.[141] For example, in 2018, *The Diplomat* noted that the Cuban government ''has been reported to sell its intercept data from U.S. communications to third-party buyers, particularly military adversaries of the [United States],'' including China.[142] Team Telecom has also found that Cuba's relationships with China and Russia—which include extensive economic, military and intelligence cooperation—heighten the risk that Cuba could share U.S. sensitive

[127] Off. of the Dir. of Nat'l Intel., *supra* note 86, at 12.

[128] Nat'l Intel. Council, *supra* note 5, at 3.

[129] Nat'l Counterintel. & Sec. Ctr., *supra* note 48, at 4; Wray, *supra* note 98.

[130] Press Release, U.S. Dep't of Treas., *Treasury Sanctions Senior Cuban Officials in Response to Violence Against Peaceful Demonstrators* (Aug. 19, 2021), *https://home.treasury.gov/news/press-releases/jy0327* [*https://perma.cc/TQP2-U79G*]; Press Statement, The White House, *Fact Sheet: Biden Harris Administration Measures on Cuba* (July 22, 2021), *https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/22/fact-sheet-biden-harris-administration-measures-on-cuba/* [*https://perma.cc/J7H7-BAA8*]; Eric Bazail-Eimil, *Record-Breaking Numbers of Cuban Migrants Entered the U.S. in 2022–23,* Politico (Oct. 24, 2023), *https://www.politico.com/news/2023/10/24/record-breaking-numbers-of-cuban-migrants-entered-the-u-s-in-2022-23-00123346* [*https://perma.cc/ZQ6C-KCC4*].

[131] Press Release, U.S. Embassy in Cuba, *U.S. Announces Designation of Cuba as a State Sponsor of Terrorism* (Jan. 11, 2021), *https://cu.usembassy.gov/u-s-announces-designation-of-cuba-as-a-state-sponsor-of-terrorism/* [*https://perma.cc/6GE4-5JJS*].

[132] *Cuba Sanctions,* U.S. Dep't of State, *https://www.state.gov/cuba-sanctions/* [*https://perma.cc/Q7S9-9XA6*].

[133] Nat'l Counterintel. & Sec. Ctr., *National Counterintelligence Strategy of the United States 2020–2022,* at 2 (Jan. 7, 2020), *https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf* [*https://perma.cc/V8NU-PN23*].

[134] Press Release, U.S. Dep't of Just., *Former U.S. Ambassador and National Security Council Official Admits to Secretly Acting as Agent of the Cuban Government and Receives 15-Year Sentence* (Apr. 12, 2024), *https://www.justice.gov/opa/pr/former-us-ambassador-and-national* security-council-official-admits-secretly-acting-agent [*https://perma.cc/NU9F-6NUS*]; Complaint, *United States* v. *Rocha,* No. 23–mj–04368 (S.D. Fla. filed Dec. 4, 2023).

[135] Press Release, U.S. Dep't of Just., *Former State Department Official Sentenced to Life in Prison for Nearly 30-Year Espionage Conspiracy* (July 16, 2010), *https://www.justice.gov/opa/pr/former-state-department-official-sentenced-life-prison-nearly-30-year-espionage-conspiracy* [*https://perma.cc/622F-Y6NR*].

[136] Press Release, U.S. Dep't of Just., *Unsealed Indictment Charges Former U.S. Federal Employee with Conspiracy to Commit Espionage for Cuba* (Apr. 25, 2013), *https://www.justice.gov/opa/pr/unsealed-indictment-charges-former-us-federal-employee-conspiracy-commit-espionage-cuba* [*https://perma.cc/ZSW8-7A4R*]; Indictment ¶¶ 14–34, *United States* v. *Velazquez,* No. 04–cr–044 (D.D.C. filed Feb. 5, 2004), ECF No. 1.

[137] *Ana Montes: Cuban Spy, Famous Cases and Criminals,* Fed. Bureau of Investig., *https://www.fbi.gov/history/famous-cases/ana-montes-cuba-spy* [*https://perma.cc/MJJ5-WG9X*].

[138] Press Release, U.S. Dep't of Just., *Team Telecom Recommends the FCC Deny Application to Directly Connect the United States to Cuba Through Subsea Cable* (Nov. 30, 2022), *https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-deny-application-directly-connect-united-states-cuba-through* [*https://perma.cc/J7RF-HM6U*]; *see generally* ARCOS–1 USA, Inc., File No. SCL–MOD–202100928–0039 (Fed. Commc'ns Comm'n Nov. 29, 2022) (committee recommendation to deny application), *https://www.justice.gov/opa/file/1555196/dl?inline* [*https://perma.cc/F9SV-7U98*].

[139] ARCOS–1 USA, Inc., *supra* note 138, at 11–12.

[140] ARCOS–1 USA, Inc., *supra* note 138, at 14–15.

[141] *Id.* at 17–25.

[142] Victor Robert Lee, *Satellite Images: A (Worrying) Cuban Mystery,* Diplomat (June 8, 2018), *https://thediplomat.com/2018/06/satellite-images-a-worrying-cuban-mystery* [*https://perma.cc/H6ZF-P3QU*].

personal data that it obtains with China or Russia.[143]

c. Iran

The Department has determined, with the concurrence of the Secretaries of State and Commerce, that Iran has engaged in a long-term pattern of conduct significantly adverse to the national security of the United States and the security and safety of U.S. persons. Iran engages in transnational repression;[144] commits human-rights abuses, including against U.S. persons;[145] smuggles U.S. technology;[146] evades U.S. sanctions;[147] sponsors terrorism;[148] and conducts malicious cyber activities, among other conduct.

Because Iran has growing cyber expertise and aggressively seeks to obtain and exploit data on U.S. persons, it poses a significant risk of exploiting government-related data or Americans' bulk U.S. sensitive personal data to the detriment of the national security of the United States and the security and safety of U.S. persons. According to ODNI, ''Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. and allied . . . networks and data.'' [149] Individuals linked to the Iranian government engage in advanced cyber activities that target U.S. infrastructure,[150] conduct cyber espionage,[151] and steal data from U.S. persons, companies, and government agencies. For example, in 2018, a Federal grand jury returned an indictment against nine Iranians for stealing ''more than 31 terabytes of documents and data from more than 140 American universities, 30 American companies, [and] five American government agencies,'' in part at the behest of the Iranian government.[152]

In particular, Iranian hackers ''have engaged in widespread theft of personal information . . . to track targets of interest to the Iranian regime'' [153] and influence U.S. persons. During the 2020 U.S. elections, ''Iranian cyber actors obtained or attempted to obtain U.S. voter information, sent threatening emails to voters, and disseminated disinformation about the election.'' [154] According to ODNI, those same Iranian actors have developed new cyber and influence techniques that Iran could deploy during the 2024 election cycle.[155] Iran-associated individuals also target U.S. persons for assassinations. For example, in 2023, a Federal grand jury returned an indictment against three individuals for plotting the murder of a U.S. citizen targeted by Iran for speaking out against the regime's human-rights abuses.[156] In another example of Iran's exploitation of sensitive personal data, Iranian cyber threat actors engaged in ''widespread theft'' of personal information, ''probably to support surveillance operations that enable Iran's human-rights abuses.'' [157] Iranian threat actors also ''employed a years-long malware campaign'' that targeted Iranian citizens, dissidents, journalists, and foreign organizations, including U.S.-based travel services companies that possess personal information on millions of travelers.[158]

d. North Korea

The Department has determined, with the concurrence of the Secretaries of State and Commerce, that North Korea has engaged in a long-term pattern of conduct significantly adverse to the national security of the United States and the security and safety of U.S. persons. Among other conduct significantly adverse to the national security of the United States and the security and safety of U.S. persons, it develops weapons of mass destruction;[159] commits human-rights abuses, including against U.S. persons;[160] evades U.S. sanctions;[161] and conducts malicious cyber activities.

[143] ARCOS–1 USA, Inc., *supra* note 138, at 17–25.

[144] Press Statement, Matthew Miller, Spokesperson, Dep't of State, *Taking Actions to Combat the Iranian Regime's Transnational Repression* (Jan. 29, 2024), *https://www.state.gov/taking-actions-to-combat-the-iranian-regimes-transnational-repression/* [*https://perma.cc/VS2Z-VA32*].

[145] Press Statement, Antony J. Blinken, Sec'y, Dep't of State, *Designating Iranian Persons Connected to Wrongful Detentions* (Sept. 18, 2023), *https://www.state.gov/designating-iranian-persons-connected-to-wrongful-detentions/* [*https://perma.cc/2CFT-YQWB*].

[146] Press Statement, Matthew Miller, Spokesperson, Dep't of State, *Designating Persons Tied to Network Smuggling U.S. Technology to Central Bank of Iran* (Feb. 14, 2024), *https://www.state.gov/designating-persons-tied-to-network-smuggling-u-s-technology-to-central-bank-of-iran/* [*https://perma.cc/XD7P-JKNU*].

[147] Press Release, U.S. Dep't of Treas., *Treasury Targets Sanctions Evasion Network Moving Billions for Iranian Regime* (Mar. 9, 2023), *https://home.treasury.gov/news/press-releases/jy1330* [*https://perma.cc/U8J2-NZ5Y*]; Press Release, U.S. Dep't of Just., *Justice Department Announces Terrorism and Sanctions-Evasion Charges and Seizures Linked to Illicit, Billion-Dollar Global Oil Trafficking Network that Finances Iran's Islamic Revolutionary Guard Corps and Its Malign Activities* (Feb. 2, 2024), *https://www.justice.gov/opa/pr/justice-department-announces-terrorism-and-sanctions-evasion-charges-and-seizures-linked* [*https://perma.cc/AXS4-63QM*]; Indictment ¶ 2, *United States* v. *Shahriyari,* No. 24–cr–44 (S.D.N.Y. filed Jan. 25, 2024), ECF No. 1, *https://www.justice.gov/opa/media/1336966/dl?inline* [*https://perma.cc/T664-3F6U*].

[148] U.S. Dep't of Just., *supra* note 147.

[149] Off. of the Dir. of Nat'l Intel., *supra* note 86, at 20.

[150] Cybersec. & Infrastructure Sec. Agency, AA21–321A, *Cybersecurity Advisory: Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities* (Nov. 19, 2021), *https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-321a* [*https://perma.cc/9F3H-KY7F*].

[151] Cybersec. & Infrastructure Sec. Agency, *Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks* (Feb. 24, 2022), *https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-055a* [*https://perma.cc/46ZR-MDVN*].

[152] Press Release, U.S. Dep't of Just., *Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps* (Mar. 23, 2018), *https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary* [*https://perma.cc/F3BP-GJP7*].

[153] Nat'l Intel. Council, *supra* note 5, at 4.

[154] Off. of the Dir. of Nat'l Intel., *supra* note 86, at 20.

[155] *Id.* at 20.

[156] Press Release, U.S. Dep't of Just., *Justice Department Announces Charges and New Arrest in Connection with Assassination Plot Directed from Iran* (Jan. 27, 2023), *https://www.justice.gov/opa/pr/justice-department-announces-charges-and-new-arrest-connection-assassination-plot-directed* [*https://perma.cc/WW34-K9AH*]; *Iran Sanctions,* U.S. Dep't State, *https://www.state.gov/iran-sanctions/* [*https://perma.cc/MH6Z-EFV7*]; *see also* Press Release, U.S. Dep't of Just., *One Iranian and Two Canadian Nationals Indicted in Murder-for-Hire Scheme* (Jan. 29, 2024), *https://www.justice.gov/opa/pr/one-iranian-and-two-canadian-nationals-indicted-murder-hire-scheme* [*https://perma.cc/2DDC-Q7VQ*]; Press Release, U.S. Dep't of Treas., *The United States and United Kingdom Target Iranian Transnational Assassinations Network* (Jan. 29, 2024), *https://home.treasury.gov/news/press-releases/jy2052* [*https://perma.cc/SE4A-7G4U*].

[157] Press Release, U.S. Dep't of Treas., *Treasury Sanctions Iranian Ministry of Intelligence and Minister for Malign Cyber Activities* (Sept. 9, 2022), *https://home.treasury.gov/news/press-releases/jy0941* [*https://perma.cc/98LB-5XYJ*].

[158] Press Release, Fed. Bureau of Investig., *FBI Releases Cybersecurity Advisory on Previously Undisclosed Iranian Malware Used to Monitor Dissidents and Travel and Telecommunications Companies* (Sept. 17, 2020), *https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-releases-cybersecurity-advisory-on-previously-undisclosed-iranian-malware-used-to-monitor-dissidents-and-travel-and-telecommunications-companies* [*https://perma.cc/K8V5-LA6U*].

[159] Press Statement, Antony J. Blinken, Sec'y, Dep't of State, *Designation of Two DPRK Individuals Supporting the DPRK's Unlawful Weapons of Mass Destruction and Missile Programs* (June 15, 2023), *https://www.state.gov/designation-of-two-dprk-individuals-supporting-the-dprks-unlawful-weapons-of-mass-destruction-and-missile-programs/* [*https://perma.cc/EV6L-3TCL*].

[160] Press Release, U.S. Dep't of Treas., *Treasury Sanctions Over 40 Individuals and Entities Across Nine Countries Connected to Corruption and Human Rights Abuse* (Dec. 9, 2022), *https://home.treasury.gov/news/press-releases/jy1155* [*https://perma.cc/Y6ST-UVSP*]; Bernd Debusmann Jr., *What Happened to US Citizens Like Otto Warmbier Detained in North Korea,* BBC News (July 18, 2023), *https://www.bbc.com/news/world-us-canada-66236989* [*https://perma.cc/MTL8-D425*].

[161] Press Statement, Antony J. Blinken, Sec'y, Dep't of State, *The Democratic People's Republic of Korea's Illicit Activities and Sanctions Evasion*

Continued

Regarding North Korea's malicious cyber activities, ODNI has concluded that North Korea's cyber program poses a ''sophisticated and agile espionage, cybercrime, and attack threat,'' and that North Korea's cyber forces are ''fully capable of achieving a variety of strategic objectives against diverse targets'' in the United States.[162]

Because North Korea has sophisticated cyber capabilities and attempts to obtain and exploit data on U.S. persons, it poses a significant risk of exploiting government-related data or Americans' bulk U.S. sensitive personal data to the detriment of the national security of the United States and the security and safety of U.S. persons. North Korea conducts cyber-enabled attacks and steals personal information to influence and target U.S. persons. For example, in 2014, North Korea-affiliated hackers attacked U.S. company Sony Pictures Entertainment in retaliation for an American film depicting the North Korean leader.[163] They stole proprietary information, personally identifiable information, and confidential communications; rendered Sony Pictures Entertainment's computers inoperable; and threatened the company's executives and employees.[164] North Korea and North Korea-affiliated hacker groups have repeatedly targeted military networks, critical infrastructure, and other corporate networks to ''steal data and conduct disruptive and destructive cyber activities.'' [165] For example, in 2017, North Korea was responsible for a massive ransomware attack that infected hundreds of thousands of computers in more than 150 countries.[166] North Korea also ''uses cyber capabilities to steal from financial institutions'' and ''generate revenue for its weapons of mass destruction and ballistic missile programs.'' [167] North Korea's cyber actors use a range of tactics ''to further their larger espionage and financial goals,'' including conducting spear phishing, abusing privileged access to networks while working as information technology contractors, exploiting software vulnerabilities, and attacking supply chains.[168] North Korea is also trying to use AI to further its offensive cyber capabilities.[169]

e. Russia

The Department has determined, with the concurrence of the Secretaries of State and Commerce, that Russia has engaged in a long-term pattern of conduct significantly adverse to the national security of the United States and the security and safety of U.S. persons. According to ODNI, Russia poses ''an enduring global cyber threat'' and views ''cyber disruptions as a foreign policy lever to shape other countries' decisions.'' [170] Russia has launched a ''full-scale war against Ukraine;'' [171] commits human-rights abuses, including against U.S. persons; [172] conducts malign influence campaigns; [173] evades U.S. sanctions; [174] and conducts malicious cyber activities.[175] Russia ''continuously refines and employs its espionage, influence, and attack capabilities'' against a variety of targets, including critical infrastructure in the United States.[176] For example, in 2019, Russian intelligence services perpetrated a ''broad-scope cyber espionage campaign'' that exploited the SolarWinds Orion platform and compromised both United States Government agencies and private-sector organizations.[177] The campaign gave Russian intelligence ''the ability to spy on or potentially disrupt more than 16,000 computer systems worldwide.'' [178] Russian intelligence ultimately used the attack to target United States Government agencies and employees for espionage.[179]

Because Russia has advanced cyber capabilities and aggressively seeks to obtain and exploit data on U.S. persons, including to conduct influence campaigns in the United States, it poses a significant risk of exploiting government-related data or Americans' bulk U.S. sensitive personal data to the detriment of the national security of the United States and the security and safety of U.S. persons. Russia engages in the large-scale theft of sensitive personal data and is ''increasing [its] ability to analyze and manipulate large quantities of personal information,'' enabling it ''to more effectively target and influence, or coerce, individuals and groups in the

(May 6, 2022), *https://www.state.gov/the-democratic-peoples-republic-of-koreas-illicit-activities-and-sanctions-evasion/* [*https://perma.cc/LQ9B-9Z22*].

[162] Off. of the Dir. of Nat'l Intel., *supra* note 86, at 22.

[163] Press Release, U.S. Dep't of Just., *North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions* (Sept. 6, 2018), *https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and* [*https://perma.cc/WXQ3-YMQA*].

[164] Press Release, Fed. Bureau of Investig., *Update on Sony Investigation* (Dec. 19, 2014), *https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation* [*https://perma.cc/5H4K-5EFV*].

[165] Cybersec. & Infrastructure Sec. Agency, *Guidance on the North Korean Cyber Threat* (June 23, 2020), *https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-106a* [*https://perma.cc/X8CJ-TAYV*].

[166] U.S. Dep't of Just., *supra* note 163.

[167] Cybersec. & Infrastructure Sec. Agency, *supra* note 165.

[168] Off. of the Dir. of Nat'l Intel., *North Korean Tactics, Techniques and Procedures for Revenue Generation* (July 2023), *https://www.dni.gov/files/CTIIC/documents/products/North-Korean-TTPs-for-Revenue-Generation.pdf* [*https://perma.cc/Y949-JJW4*]; Press Release, U.S. Dep't of Just., *Justice Department Announces Court-Authorized Action to Disrupt Illicit Revenue Generation Efforts of Democratic People's Republic of Korea Information Technology Workers* (Oct. 18, 2023), *https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-action-disrupt-illicit-revenue-generation* [*https://perma.cc/3JHY-UH5K*].

[169] Anne Neuberger, Deputy Nat'l Sec. Advisor for Cyber & Emerging Tech., Nat'l Sec. Council, U.S. Dep't of State, Digital Press Briefing (Oct. 18, 2023), *https://www.state.gov/digital-press-briefing-with-anne-neuberger-deputy-nationalsecurity-advisor-for-cyber-and-emerging-technologies/* [*https://perma.cc/GK88-FW8H*].

[170] Off. of the Dir. of Nat'l Intel., *supra* note 86, at 16; *see also* Press Statement, The White House, *Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government* (Apr. 15, 2021), *https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/* [*https://perma.cc/MD56-GD27*]; Nat'l Counterintel. & Sec. Ctr., *SolarWinds Orion Software Supply Chain Attack* (Aug. 19, 2021), *https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/SolarWinds%20Orion%20Software%20Supply%20Chain%20Attack.pdf* [*https://perma.cc/TS3M-MQQ7*].

[171] Press Statement, Antony J. Blinken, Sec'y, Dep't of State, *Responding to Two Years of Russia's Full-Scale War Against Ukraine and Aleksey Navalny's Death* (Feb. 23, 2024), *https://www.state.gov/responding-to-two-years-of-russias-full-scale-war-against-ukraine-and-aleksey-navalnys-death/* [*https://perma.cc/K3SL-LHFF*].

[172] Press Statement, Vedant Patel, Principal Deputy Spokesperson, Dep't of State, *Russia's Wrongful Detention of Journalist Evan Gershkovich* (Apr. 10, 2023), *https://www.state.gov/russias-wrongful-detention-of-journalist-evan-gershkovich/* [*https://perma.cc/XE2R-93RE*].

[173] Press Release, U.S. Dep't of Treas., *Treasury Sanctions Actors Supporting Kremlin-Directed Malign Influence Efforts* (Mar. 20, 2024), *https://home.treasury.gov/news/press-releases/jy2195* [*https://perma.cc/TB2X-YRPN*]; Press Release, U.S. Dep't of Treas., *Treasury Targets the Kremlin's Continued Malign Political Influence Operations in the U.S. and Globally* (July 29, 2022), *https://home.treasury.gov/news/press-releases/jy0899* [*https://perma.cc/FXN8-J748*].

[174] Press Release, U.S. Dep't of Treas., *Treasury Targets Sanctions Evasion Networks and Russian Technology Companies Enabling Putin's War* (Mar. 31, 2022), *https://home.treasury.gov/news/press-releases/jy0692* [*https://perma.cc/ERD6-ARTE*].

[175] Press Statement, Matthew Miller, Spokesperson, Dep't of State, *U.S. Takes Action to Further Disrupt Russian Cyber Activities* (Dec. 7, 2023), *https://www.state.gov/u-s-takes-action-to-further-disrupt-russian-cyber-activities/* [*https://perma.cc/AW9F-E8BP*].

[176] Off. of the Dir. of Nat'l Intel., *supra* note 86, at 16.

[177] White House, *supra* note 170.

[178] *Id.*

[179] *SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic),* U.S. Gov't Accountability Off. (Apr. 22, 2021), *https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic* [*https://perma.cc/3A2V-6S59*].

United States.'' [180] For example, in 2013, Russian intelligence services sponsored the theft of information associated with at least 500 million accounts from U.S. web services company Yahoo![181] and used some of that stolen information to obtain unauthorized access to the email accounts of United States Government officials, among others.[182] In 2020, Russian cyber operations targeted and compromised U.S. State and local government networks and exfiltrated some voter data.[183] In another example, in 2023, a Federal grand jury returned an indictment against two Russian individuals for obtaining unauthorized access to the computers and email accounts of current and former United States Government employees and stealing intelligence related to defense, security policies, and nuclear energy technology from the victims' accounts.[184] In 2024, Russian intelligence services used compromised routers to conduct ''spearphishing and similar credential harvesting campaigns against targets of intelligence interest to the Russian government, such as U.S. and foreign governments and military, security, and corporate organizations.'' [185]

Russia also has a legal regime that gives it the capability to covertly access and exploit data through companies subject to its jurisdiction. As the Department of Commerce has explained, ''Russian laws compel companies subject to Russian jurisdiction to cooperate with Russian intelligence and law enforcement efforts, to include requests from the Russian Federal Security Service (''FSB'').'' [186] These laws include the following:

- Federal Law No. 40–FZ of April 3, 1995, ''On the Federal Security Service,'' ''requires FSB bodies to carry out their activities in collaboration with various entities in Russia'' and places private enterprises ''under a legal obligation to assist FSB bodies in the execution of the duties assigned to FSB bodies,'' including intelligence and counterintelligence activities.[187]
- Federal Law No. 144–EZ of August 12, 1995 (as amended), ''On Operational-Investigative Activity,'' requires persons subject to Russian jurisdiction to ''assist the FSB with operational-investigative activities undertaken in the performance of FSB duties, such as by installing equipment supplied by the FSB for use in obtaining information stored on computers.'' [188] This law ''makes it clear that, as a general rule, operational-investigative activities may be carried out against anyone anywhere'' and ''makes it clear that operational-search activities include obtaining computer information.'' [189]
- Federal Law No. 149–FZ of July 27, 2006, ''On Information, Information Technologies, and Protection of Information,'' imposes several ''obligations on any entity that qualifies as 'an organizer of the dissemination of information on the internet,' '' which is broadly defined to include any ''person who carries out activities to ensure the operation of information systems and/or programs for electronic computers that are designed and/or used to receive, transmit, deliver and/or process electronic messages of users of the internet.'' [190] These obligations include giving the FSB and other Russian agencies in the field of security ''the information necessary to decode'' encrypted data.[191]

In short, persons subject to Russia's jurisdiction must ''assist the FSB in its counterintelligence and intelligence functions,'' which ''includes a duty to assist the FSB in operational-investigative activity, in support of FSB counterintelligence and intelligence functions'' such as ''collecting information from U.S. computers,'' ''with no need for the FSB to have obtained a court order.'' [192]

Finally, Russia also poses a ''serious foreign influence threat because of its wide-ranging efforts to . . . sow domestic discord, including among voters inside the United States.'' [193] In July 2018, a Federal grand jury returned an indictment against Russian intelligence officers after they conducted a spear phishing campaign against volunteers and employees of a presidential campaign and political committees.[194] The actors hacked into computers, stole emails, covertly monitored the computer activity of campaign employees, and released the hacked information to the public in an attempt to interfere with the 2016 U.S. presidential election.[195]

f. Venezuela

The Department has determined, with the concurrence of the Secretaries of State and Commerce, that Venezuela has engaged in a long-term pattern of conduct significantly adverse to the national security of the United States and the security and safety of U.S. persons. Among other conduct significantly adverse to the national security of the United States and the security and safety of U.S. persons, Venezuela commits human-rights abuses, including against U.S. persons; [196] evades U.S. sanctions; [197] has concerning relationships with other

[180] Nat'l Intel. Council, *supra* note 5, at 3.

[181] Press Release, U.S. Dep't of Just., *U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts* (Mar. 15, 2017), *https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions* [*https://perma.cc/44UK-XM7P*].

[182] U.S. Dep't of Just., *supra* note 181; Indictment ¶ 34, *United States* v. *Dokuchaev,* No. 17-cr-103 (N.D. Cal. filed Feb. 28, 2017).

[183] Nat'l Intel. Council, ICA 2020–00078D, *Intelligence Community Assessment on Foreign Threats to the 2020 US Federal Elections* 3 (Mar. 10, 2021), *https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf* [*https://perma.cc/R8LM-KEUX*].

[184] Indictment ¶¶ 3–5, *United States* v. *Aleksandrovic,* No. 23–cr–447 (N.D. Cal. filed Dec. 5, 2023).

[185] Press Release, U.S. Dep't of Just., *Justice Department Conducts Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate of the General Staff (GRU)* (Feb. 15, 2024), *https://www.justice.gov/opa/pr/justice-department-conducts-court-authorized-disruption-botnet-controlled-russian* [*https://perma.cc/8M8Z-C3SM*].

[186] Kaspersky Lab, Inc., *supra* note 20, 89 FR 52435.

[187] Report of Peter B. Maggs to the U.S. Dep't of Homeland Sec. ¶¶ 14–18 (Dec. 2, 2017), *https://www.internetgovernance.org/wp-content/uploads/12-7-Exhibit-AR-Part-6-Maggs-report.pdf* [*https://perma.cc/US4P-VMCP*] (hereinafter ''Maggs Report'') (supporting the Department of Homeland Security's Dec. 4, 2017 Final Decision on Binding Operational Directive 17–01, Removal of Kaspersky-Branded Products).

[188] Kaspersky Lab, Inc., *supra* note 20, 89 FR 52435 n.13; Maggs Report, *supra* note 187, ¶¶ 24–25.

[189] Maggs Report, *supra* note 187, ¶¶ 24–29.

[190] *Id.* ¶ 21.

[191] *Id.* ¶¶ 13(f), 31.

[192] *Id.* ¶ 30.

[193] Off. of the Dir. of Nat'l Intel., *supra* note 86, at 17.

[194] Press Release, U.S. Dep't of Just., *Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election* (July 13, 2018), *https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election* [*https://perma.cc/RG2P-SJLQ*]; Indictment ¶¶ 2–5, *United States* v. *Netyksho,* No. 18–cr–215 (D.D.C. filed July 13, 2018).

[195] U.S. Dep't of Just., *supra* note 194; Indictment ¶¶ 2–5, *Netyksho,* No. 8–cr–215.

[196] U.S. Dep't of State, *2022 Country Reports on Human Rights Practices: Venezuela* (2022), *https://www.state.gov/wp-content/uploads/2023/02/415610_VENEZUELA-2022-HUMAN-RIGHTS-REPORT.pdf* [*https://perma.cc/7TM9-P87S*]; *see also, e.g.,* E.O. 13692, 80 FR 12747 (Mar. 8, 2015).

[197] Press Release, U.S. Att'ys Off. DC, U.S. Dep't of Just., *Largest U.S. Seizure of Iranian Fuel from Four Tankers* (Aug. 14, 2020), *https://www.justice.gov/usao-dc/pr/largest-us-seizure-iranian-fuel-four-tankers* [*https://perma.cc/66EF-42CD*]; Fin. Crimes Enf't Network, U.S. Dep't of Treas., FIN–2019–A002, *Updated Advisory on Widespread Public Corruption in Venezuela,* 8 (May 3, 2019), *https://www.fincen.gov/sites/default/files/advisory/2019-05-03/Venezuela%20Advisory%20FINAL%20508.pdf* [*https://perma.cc/X5VL-HH69*].

countries of concern;[198] and fosters widespread corruption.[199]

Because Venezuela exploits its demonstrated and systematic relationships with other countries of concern to degrade U.S. national security; aggressively surveils its own population to target perceived government critiques, including with the help of other countries of concern; and, according to credible reports, commits human-rights abuses, including against U.S. citizens, Venezuela's access to government-related data or Americans' bulk U.S. sensitive personal data poses a significant risk to the national security of the United States and the security and safety of U.S. persons. Regarding Venezuela's human-rights abuses, Venezuela surveils its domestic population through telecommunications providers to target perceived opponents, including with the help of other countries of concern.[200] Venezuela's misuse of private telecommunications capabilities for expansive surveillance poses risks to U.S. persons, as the regime has the capability to access data on U.S. persons in Venezuela. For example, in 2021, a report by Spanish telecommunications company Telefonica revealed that Venezuela monitored the communications of nearly 1.5 million of its users, which represents over 20 percent of Telefonica's Venezuela-based customers.[201] In addition to surveillance, there are credible reports that Venezuela perpetrates extensive human-rights abuses, such as torture, extrajudicial killings, and enforced disappearances. Venezuelan security forces detain individuals, including U.S. citizens, for long periods without due process.[202] According to the State Department, the United States Government is not generally notified of the detention of U.S. citizens in Venezuela or granted access to U.S. citizen prisoners in Venezuela.[203]

Venezuela maintains close relationships with other countries of concern that, as described in part IV.D of this preamble, possess sophisticated surveillance capabilities and pose a significant risk of exploiting government-related data or Americans' bulk U.S. sensitive personal data. Given the nature of these relationships, Venezuela might use technology provided by these countries of concern to obtain access to government-related data or bulk U.S. sensitive personal data, or share any access to government-related data or bulk U.S. sensitive personal data with these countries of concern. For example, Venezuela uses equipment provided by Chinese technology company Zhongxing Telecommunication Equipment (''ZTE'') Corporation, which the FCC has designated a national security threat to the U.S. communications network and supply chain, to monitor Venezuelan citizens' social, political, and economic activities.[204] The company has provided Venezuela with identity cards, referred to as ''carnet de la patria'' or ''fatherland cards,'' that the regime can use to track citizen behavior.[205] Additionally, Venezuelan and Russian state-owned companies jointly own Evrofinance Mosnarbank, a bank that has financed Venezuela's efforts to use digital currencies to circumvent U.S. financial sanctions.[206] Evrofinance Mosnarbank also provides financial support to Petroleos de Venezuela, a Venezuelan state-owned oil company that has been used to embezzle and launder billions of dollars.[207] Venezuela also has concerning military and intelligence ties with other countries of concern. For example, Russia provides military support to Venezuela.[208] Cuba provides training to Venezuelan intelligence and military personnel, and the two nations support each other's intelligence operations.[209]

E. Subpart G—Covered Persons

1. Section 202.211—Covered Person

The proposed rule identifies a ''covered person'' as an individual or entity that falls into one of the classes of covered persons or that the Attorney General has designated as a covered person. An entity is a covered person if it is a foreign person that: (1) is 50 percent or more owned, directly or indirectly, by a country of concern; (2) is organized or chartered under the laws of a country of concern; or (3) has its principal place of business in a country of concern. An entity is also a covered person if it is a foreign person that is 50-percent or more owned, directly or indirectly, by a covered person. Any foreign individual who is an employee or a contractor of such an entity or of the country of concern itself is also a covered person. Any foreign person who is primarily a resident in the territorial jurisdiction of a country of concern is also a covered person.

The proposed rule would not categorically treat citizens of countries of concern located in third countries (*i.e.,* not located in the United States and not primarily resident in a country of concern) as covered persons. Instead, it treats only a subset of country of concern citizens in third countries categorically as covered persons: those working for the government of a country of concern or for an entity that is a covered person. All other country of concern citizens located in third countries would not qualify as covered persons except to the extent that the Attorney General designates them.

Some commenters believed that it would be difficult for U.S. persons

[198] U.S. Dep't of Just., *supra* note 197; Off. of the Dir. of Nat'l Intel., *supra* note 86, at 29.

[199] Press Release, U.S. Dep't of Just., *Former Venezuelan National Treasurer and Her Husband Sentenced in Money Laundering and International Bribery Scheme* (Apr. 19, 2023), *https://www.justice.gov/opa/pr/former-venezuelan-national-treasurer-and-her-husband-sentenced-money-laundering-and* [*https://perma.cc/AU8N-C9UD*]; Fin. Crimes Enf't Network, *supra* note 197, at 7.

[200] U.S. Dep't of State, *supra* note 196, at 19; María Luisa Paúl, *Venezuela Tapped 1.5 Million Phone Lines. It's Just the Start, Experts Warn.,* Wash. Post (June 28, 2022), *https://www.washingtonpost.com/nation/2022/06/28/telefonica-wiretapping-venezuela-phone/* [*https://perma.cc/T8YV-A9TW*].

[201] U.S. Dep't of State, *supra* note 196, at 19; Paúl, *supra* note 200.

[202] U.S. Dep't of State, *Venezuela Travel Advisory* (May 13, 2024), *https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories/venezuela-travel-advisory.html* [*https://perma.cc/5F26-GNRM*]; Clare Ribando Seelke et al., Cong. Rsch. Serv., R44841, *Venezuela: Background and U.S. Relations* 7 (Dec. 6, 2022), *https://crsreports.congress.gov/product/pdf/R/R44841* [*https://perma.cc/T8ZW-4RRA*].

[203] U.S. Dep't of State, *supra* note 196.

[204] FCC, Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs—ZTE Designation, 35 FCC Rcd. 6633 (2020), *https://docs.fcc.gov/public/attachments/DA-20-691A1.pdf* [*https://perma.cc/MK3W-SYEN*].

[205] Angus Berwick, *How ZTE Helps Venezuela Create China-Style Social Control,* Reuters (Nov. 14, 2018), *https://www.reuters.com/investigates/special-report/venezuela-zte/* [*https://perma.cc/66X9-FBWD*]; *see also* U.S. Dep't of State, *supra* note 196.

[206] Fin. Crimes Enf't Network, *supra* note 197, at 4–5.

[207] *Id.;* Press Release, U.S. Dep't of Treas., *Treasury Sanctions Venezuela's State-Owned Oil Company Petroleos de Venezuela, S.A.* (Jan. 28, 2019), *https://home.treasury.gov/news/press-releases/sm594* [*https://perma.cc/375J-DR47*].

[208] Regina Garcia Cano, *Venezuela's Leader Pledges Military Cooperation with Russia,* AP News (Feb. 16, 2022), *https://apnews.com/article/europe-russia-venezuela-vladimir-putin-south-america-fc9e01895f52f8d9f52e501a93b2f089* [*https://perma.cc/M59U-SRUU*]; *Russia in the Western Hemisphere: Assessing Putin's Malign Influence in Latin America and the Caribbean: Hearing Before the H. Foreign Affs. Subcomm. on W. Hemisphere, Civilian Sec., Migration, & Int'l Econ. Pol'y,* 117th Cong. 1–3 (2022) (statement of Evan Ellis, Senior Associate, Ctr. for Strategic & Int'l Stud.), *https://csis-website-prod.s3.amazonaws.com/s3fs-public/congressional_testimony/ts220720_Ellis.pdf* [*https://perma.cc/K9VG-ZFW2*].

[209] Moises Rendon & Claudia Fernandez, Ctr. for Strategic & Int'l Stud., *The Fabulous Five: How Foreign Actors Prop Up the Maduro Regime in Venezuela* 7 (2020), *https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/201019_Rendon_Venezuela_Foreign_Actors.pdf* [*https://perma.cc/39AG-LAAX*].

subject to the proposed rule to determine whether entities are 50 percent or more owned by countries of concern, particularly where the foreign companies are publicly traded companies. However, this provision is not unique to the proposed rule. It is similar to sanctions regulations issued by the Office of Foreign Assets Control (''OFAC'') within the Department of the Treasury. Such regulations treat any entity owned in the aggregate, directly or indirectly, 50-percent or more by one or more blocked persons as itself a blocked person, regardless of whether the entity itself is designated pursuant to an Executive Order or otherwise identified on OFAC's Specially Designated Nationals and Blocked Persons List.[210] The proposed rule also uses higher ownership thresholds than some regulatory regimes, such as those related to anti-money laundering, which generally require certain companies to identify beneficial owners with 25 percent or more (and, in some cases, 10 percent or more) direct or indirect legal interest in an entity and to collect, verify, and report specific information about them.[211] As other commenters pointed out, businesses and third-party service providers have developed tools and services to assist with screening and due diligence based on corporate ownership in the sanctions, anti-money laundering, and other regulatory contexts. Consequently, the proposed rule adopts the approach described in the ANPRM without change.

One commenter recommended that the Department clarify how the proposed rule would apply to companies headquartered outside a country of concern but with business operations in a country of concern. The proposed rule maintains the framework described in the ANPRM without change, and the Department has provided some additional examples in the proposed rule to demonstrate how the proposed rule treats foreign branches and subsidiaries located in countries of concern. *See* § 202.256(b)(5)(8). The proposed rule also exempts corporate group transactions that are ordinarily incident to and part of administrative or ancillary business operations, such as human resources, including between U.S. entities and their foreign subsidiaries or affiliates.

Several commenters suggested that the Department rely solely on designations and adopt an exclusively list-based approach to the identification of covered persons (similar to OFAC's Specially Designated Nationals and Blocked Persons List or the Bureau of Industry and Security's (''BIS'') Entity List) rather than applying the prohibitions and restrictions to categories of covered persons supplemented by a non-exhaustive list. The Department declines to adopt the exclusively list-based approach. Such an approach would be inconsistent with the Order, as well as with the national security risk associated with country of concern access to government-related data or bulk U.S. sensitive personal data. Specifically, the national security risk identified in the Order exists with respect to any entity that is subject to the ownership, direction, jurisdiction, or control of a country of concern due to the fact that each of the listed countries of concern in the proposed rule have legal or political systems that allow the countries to obtain sensitive personal data (and access to such data) from persons subject to their ownership, direction, jurisdiction, or control without due process or judicial redress.[212] That risk exists with respect to any person that is meaningfully subject to their ownership, direction, jurisdiction, or control—not only to specific entities designated on a case-by-case basis. Entities that are meaningfully subject to the ownership, direction, jurisdiction, or control of a country of concern are, as the FBI has described, hybrid commercial threats. As the FBI has explained, ''[h]ybrid [c]ommercial [t]hreats are businesses whose legitimate commercial activity can facilitate foreign government access to U.S. data, critical infrastructure, and emerging technologies that enable adversaries to conduct espionage, technology transfer, data collection, and other disruptive activities under the disguise of an otherwise legitimate commercial activity.'' [213]

As such, trying to apply a list-based approach would be insufficient to mitigate the national security risk identified in the Order and the proposed rule. The categories of covered persons defined in the Order and defined further in the proposed rule identify categories of persons that are meaningfully subject to the ownership, direction, jurisdiction of a country of concern, or control of a country of concern or covered person, and thus present this risk. Processes like those used by OFAC to add blocked persons to the Specially Designated Nationals and Blocked Persons List or by BIS to add entities to the Entity List, which are generally based on a particularized inquiry into whether the target meets the applicable legal criteria for designation,[214] would thus be

[210] *See generally* OFAC, U.S. Dep't of Treas., *Revised Guidance on Entities Owned by Persons Whose Property and Interests in Property Are Blocked* (Aug. 13, 2014), *https://ofac.treasury.gov/media/6186/download?inline* [*https://perma.cc/Q87V-VZJQ*].

[211] *See generally Beneficial Ownership Information: Frequently Asked Questions,* Fin. Crimes Enf't Network, *https://www.fincen.gov/boi-faqs* [*https://perma.cc/Z7KQ-PN79*].

[212] Nat'l Counterintel. & Sec. Ctr., *supra* note 83, at 1; Justin Sherman, *Russia Is Weaponizing Its Data Laws Against Foreign Organizations,* Brookings Inst. (Sept. 27, 2022), *https://www.brookings.edu/articles/russia-is-weaponizing-its-data-laws-against-foreign-organizations/* [*https://perma.cc/ATU2-SU3G*]; U.S. Dep't of State, *supra* note 196, at 19; *see generally Freedom in the World 2024: North Korea,* Freedom House, *https://freedomhouse.org/country/north-korea/freedom-world/2024* [*https://perma.cc/5PAA-YMQ4*]; *Freedom on the Net 2022: Cuba,* Freedom House, *https://freedomhouse.org/country/cuba/freedom-net/2022* [*https://perma.cc/FFF6-ALCB*]; Data Security Business Advisory, *Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China,* U.S. Dep't of Homeland Sec. (Dec. 22, 2020), *https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf* [*https://perma.cc/B6XM-8G9V*]; Anna Borshchevskaya, '*Brave New World': Russia's New Anti-Terrorism Legislation,* Wash. Inst. (July 8, 2016), *https://www.washingtoninstitute.org/policy-analysis/brave-new-world-russias-new-anti-terrorism-legislation* [*https://perma.cc/2XXZ-UTC7*]; *Combating the Iranian Cyber Threat: Republic at the Center of Cyber Crime Charges in Three Cases,* Fed. Bureau of Investig. (Sept. 18, 2020), *https://www.fbi.gov/news/stories/iran-at-center-of-cyber-crime-charges-in-three-cases-091820* [*https://perma.cc/DYL5-WXUC*]; Amelia Williams, *Cuba: New data protection law—what you need to know,* Data Guidance (Sept. 2022), *https://www.dataguidance.com/opinion/cuba-new-data-protection-law-what-you-need-know* [*https://perma.cc/JH83-6P7S*]; Joanna Robin, *Maduro regime doubles down on censorship and repression in lead-up to Venezuelan election,* ICIJ (July 24, 2024), *https://www.icij.org/inside-icij/2024/07/maduro-regime-doubles-down-on-censorship-and-repression-in-lead-up-to-venezuelan-election/* [*https://perma.cc/6TBD-4J28*]; U.S. Dep't of State, Bureau of Democracy, H.R. and Lab., 2021 Country Reports on Human Rights Practices: North Korea (2021), *https://www.state.gov/wp-content/uploads/2022/03/313615_KOREA-DEM-REP-2021-HUMAN-RIGHTS-REPORT.pdf* [*https://perma.cc/GF5Z-25UG*]; *Freedom on the Net 2024: Iran,* Freedom House, at C4 and C6, *https://freedomhouse.org/country/iran/freedom-net/2024* [*https://perma.cc/2QKR-9E7C*].

[213] *In Camera, Ex Parte* Classified Decl. of Kevin Vorndran, Assistant Dir., Counterintel. Div., Fed. Bureau of Invest., Doc. No. 2066897 at Gov't App. 33 ¶ 6, *TikTok Inc.* v. *Garland,* Case Nos. 24–1113, 24–1130, 24–1183 (D.C. Cir. July 26, 2024) (publicly filed redacted version).

[214] *See* 15 CFR 744.16 (1996) (''The Entity List (supplement No. 4 to [part 744]) identifies persons . . . reasonably believed to be involved, or to pose a significant risk of being or becoming involved, in activities contrary to the national security or foreign policy interests of the United States.''); *see also,* 31 CFR 589.201(a) (2022) (blocking the property of ''any person determined by the Secretary of the Treasury'' to, among other things, ''be responsible for or complicit in, or to have engaged in, directly or indirectly,'' actions or policies ''that undermine democratic processes or institutions in Ukraine'' or ''that threaten the peace, security, stability, sovereignty, or territorial integrity of Ukraine'' or ''[m]isappropriation of state assets of Ukraine or of an economically significant entity in Ukraine'').

insufficient by themselves to address the national security risk identified in the Order. An exclusively list-based approach could present considerable compliance and enforcement challenges. It also poses potential evasion risks, similar to those encountered by OFAC, and circumvention threats that could compromise national security. The Department has determined not to exclusively implement a list-based program to mitigate the risk that listed entities, such as corporations, would rename or reorganize themselves in a manner that avoids being subject to the framework. Therefore, the proposed rule adopts the approach described in the ANPRM without change.

One commenter suggested that the Department should not treat trustworthy entities located in countries of concern as covered persons. The Department declines to do so, and the proposed rule retains the framework described in the ANPRM without change. Regardless of the trustworthiness of entities, as explained in part IV.E.1 of this preamble, countries of concern have the legal authority or political systems to force, coerce, or influence entities in their jurisdictions to share their data and access with the government.[215]

One commenter urged the Department to narrow the definition of ''covered persons'' to exclude individuals who are temporarily in the United States but are otherwise residents of a country of concern. The proposed rule adopts the approach described in the ANPRM without change. As described in the ANPRM, including its Example 33, anyone in the United States (including temporarily in the United States) would be considered a U.S. person, and no U.S. persons (including those temporarily in the United States) would be categorically treated as covered persons.[216] A U.S. person (including a temporary traveler to the United States) would be a covered person only if they had been designated by the Department. The proposed rule adopts this proposal unchanged from the ANPRM.

Two related commenters expressed identical concerns that the definition of ''covered persons'' would require companies to discriminate based on nationality or race, particularly with respect to employees who are primarily resident in countries of concern. No change was made in response to these comments. As the Order makes clear, status as a covered person does not depend on the nationality or race of an individual, and the Order and proposed rule are directed at persons of any nationality or race who are subject to the ownership, direction, jurisdiction, or control of a country of concern. The definition of ''covered person'' categorically includes any foreign person that is primarily resident in a country of concern, regardless of their nationality or race. Likewise, the definition of ''covered person'' categorically includes any foreign person abroad who is an employee or contractor of a country of concern or a covered person that is an entity, regardless of their nationality or race. Similarly, the Department's authority to designate a specific individual as a ''covered person'' turns on a determination that the individual is subject to the control, jurisdiction, or direction of a country of concern, or is acting on behalf of or purporting to act on behalf of a country of concern or covered person, or has knowingly caused or directed a violation of the proposed rule. The definition of ''U.S. person'' is also not dependent on a person's nationality or race; it includes, for example, any person in the United States and any U.S. citizen or lawful permanent resident. For example, under the proposed rule, a country of concern citizen located in the United States is a U.S. person (unless individually designated). As a result, a U.S. person of any particular race or nationality would not be categorically treated as a covered person, and the only circumstance in which a U.S. person would be treated as a covered person is by individual designation. Consequently, the proposed rule adopts the approach described in the ANPRM without change.

Several commenters sought clarification that any U.S. subsidiary of a covered person is considered a U.S. person for purposes of these regulations. The proposed rule would not treat any U.S. person, including a U.S. subsidiary of a covered person, as a covered person unless the Department has designated the U.S. subsidiary as a covered person pursuant to the process described in the proposed rule. No U.S. person, including the U.S. subsidiary of a covered person, would be categorically treated as a covered person under the proposed rule. The proposed rule includes additional examples highlighting the differences in treatment between a U.S. subsidiary and its foreign owner, as well as between U.S. companies and their foreign branches.

2. Section 202.701—Designation of Covered Persons

The proposed rule provides for the Attorney General to publicly designate a person, whether an individual or entity, as a covered person with whom U.S. persons may not knowingly engage in a prohibited transaction, or a restricted transaction that fails to comply with the requirements of subpart D of the proposed rule, except as otherwise authorized under the proposed rule. The Department intends generally to model this process on the processes for designation under the various sanctions lists maintained by OFAC. Inclusion on the Department's Covered Persons List would have no effect on a person's inclusion on other United States Government designation lists, including lists maintained by OFAC.

The Department expects that, in many cases, designation will be unnecessary because a person will be automatically deemed a covered person by operation of the definition of ''covered person'' discussed in part IV.E.1 of this preamble. For example, an entity that is majority-owned by a country of concern would be a covered person by definition, regardless of whether the entity itself is designated by the Attorney General and included on the Department's Covered Persons List. Designation is not necessary in that circumstance and, except as otherwise authorized under the proposed rule, a U.S. person would be prohibited from knowingly engaging in a prohibited transaction, or a restricted transaction that fails to comply with the requirements of subpart D, with such an entity.

Even in these circumstances, however, the Attorney General may nonetheless designate such an entity and identify that entity as a covered person in the **Federal Register** and on a Department website. Such designation may serve to provide broader notice to U.S. persons that the entity is a covered person under the Order and the regulations. For example, the definition of ''covered person'' includes entities that are majority-owned directly or indirectly by a country of concern. In some circumstances, indirect ownership may not be readily apparent, and Attorney General designation, published in the **Federal Register**, will provide notice that the entity is a covered person. Even in the case of instances in which the covered person status of an entity is clear—such as companies that are openly organized or chartered under the laws of a country of concern or that have their principal place of business in a country of concern—designation and publication in the **Federal Register** may facilitate compliance with the prohibitions and restrictions under the Order and the regulations. Importantly, however, the public list would not

[215] *See* sources cited *infra* note 212.

[216] 89 FR 15790–91.

exhaustively include all covered persons, as any person that satisfies the criteria of the relevant definitions will be considered a covered person under the proposed rule, regardless of whether the person is also specifically identified on the public list. Under the proposed rule, for example, every company with its principal place of business in any country of concern is a ''covered person''; the Department does not intend to individually designate all such companies.

The proposed rule also authorizes the Department to designate as covered persons other individuals or entities that are not already captured by other elements of the definition. This process is modeled after other IEEPA-related designation processes and contemplates designation based on interagency consultation and consideration of any relevant sources of information (which may include classified information). Under the proposed rule, and consistent with the Order, the Department could designate as a covered person any person that is owned or controlled by or subject to the jurisdiction or direction of a country of concern, is acting on behalf of or purporting to act on behalf of a country of concern or other covered person, or is knowingly causing or directing a violation of these regulations. For example, individual citizens of a country of concern primarily residing in a third country are not generally considered to be covered persons. In specific cases, however, covered data transactions with such individuals may present an unacceptable national security risk because, for example, the individual may be subject to the direction of a country of concern. The proposed rule provides for the Attorney General to designate such an individual—or any other individual or entity that satisfies the substantive criteria in the proposed rule—as a covered person.

Under the proposed rule, designation as a covered person is effective upon the Department's announcement; a U.S. person with actual knowledge of the designated person's status would be prohibited from knowingly engaging in a covered data transaction with that person (except as otherwise authorized under the proposed rule). After publication in the **Federal Register**, the Department would infer knowledge of the designated person's status on the part of any U.S. person engaging in a covered data transaction with that person. As in the context of asset flight, designations must be immediately effective to prohibit the irreversible transfer of regulated data—and the attendant risk to national security—once a designation is announced. If there were delay, unscrupulous actors could rush to complete transactions that would soon become prohibited, thus inviting precisely the national security risk that the Order, and the designation, is intended to mitigate. Like the OFAC processes on which it is modeled, the proposed rule includes a mechanism for a person designated as a covered person to seek administrative reconsideration of the designation or removal from the list of designated covered persons on the basis of changed circumstances.

Designation as a covered person reflects the risk to national security that attaches to the designated person's relationship—whether voluntary or involuntary—with a country of concern. The definition of ''covered person,'' for example, includes any foreign person who is primarily resident in the territorial jurisdiction of a country of concern or any person who is an employee or contractor of an entity with its principal place of business in a country of concern. As a general matter, the national security risk from concluding a covered data transaction with such persons arises primarily from the potential actions of the government of the country of concern in relation to that person, not from the intent or personal characteristics of the individual.

A few commenters expressed concern that it will be difficult for businesses subject to the proposed rule to identify entities controlled by or subject to the jurisdiction of countries of concern. However, neither the ANPRM nor the proposed rule would require companies to determine whether entities are subject to the control or jurisdiction of a country of concern. Whether an entity is controlled by or subject to the jurisdiction or direction of a country of concern is part of the criteria applied by the Attorney General in designating individuals and entities as covered persons; it is not a standard to be applied by the private sector. If the Attorney General determines that an individual or entity meets the criteria for designation, the Attorney General will specifically and publicly designate that person, as addressed in the foregoing discussion, and the private sector can screen counterparties against that public list. For entities not so designated, the private sector need only consult the four other categories of covered persons discussed in part IV.E.1 of this preamble; the private sector need not conduct any inquiry into whether such an entity is controlled by or subject to the jurisdiction or direction of a country of concern. Therefore, the proposed rule adopts the approach described in the ANPRM without change.

F. Subpart H—Licensing

The Order authorizes the Attorney General, in concurrence with the Departments of State, Commerce, and Homeland Security and in consultation with other relevant agencies, to issue (including to modify or rescind) licenses authorizing a transaction that would otherwise be a prohibited transaction or a restricted transaction. The proposed rule implements this provision of the Order by providing processes for regulated parties to seek, and for the Attorney General to issue, general and specific licenses. The Department anticipates that licenses will be issued only in rare circumstances as the Attorney General deems appropriate.

1. Section 202.801—General Licenses

General licenses would be published in the **Federal Register** and could be relied upon by all relevant parties affected by a particular element of these regulations. As deemed appropriate, the Attorney General, in concurrence and consultation with other departments as required by the Order, may issue a general license permitting otherwise prohibited transactions, including pursuant to conditions specified in the license. In those instances, otherwise prohibited transactions that satisfy any applicable conditions would be permitted; there would be no requirement for a party to seek further authorization prior to concluding a transaction covered by such a license. General licenses could be issued to ease industry's transition once the proposed rules become effective by potentially, for example, authorizing orderly wind-down conditions for covered data transactions that would otherwise be prohibited by the proposed rules.

2. Section 202.802—Specific Licenses

Specific licenses, on the other hand, would cover only parties who apply to the Department for such a license and disclose the facts and circumstances of the covered data transaction they seek to engage in. Specific licenses would authorize only the transactions described in the license; a specific license might authorize one or more transactions that would otherwise be prohibited.

3. Conditions on General and Specific Licenses

Both general licenses and specific licenses could include a range of requirements or obligations as the Department deems appropriate. For example, a license might be conditioned

on additional disclosure requirements, ongoing reporting obligations, recordkeeping obligations, due diligence requirements, certification requirements, cybersecurity requirements, or inclusion of certain contractual terms. The Department believes, as a general matter, that imposing uniform requirements across licenses to the greatest extent possible will encourage adoption of those practices as a matter of course and will facilitate compliance for parties operating under more than one license. For example, recordkeeping requirements for one license might be identical to those of another license. Nonetheless, the Department believes that it is important to retain flexibility in crafting applicable requirements—especially in the context of specific licenses—to account for varying contexts of the contemplated transactions and other aspects of the license at issue. The proposed rule reflects that flexibility.

The authorization provided by a license is contingent on satisfying all conditions of the license. Transactions not conducted in compliance with a license's conditions would be subject to the regulation's restrictions and prohibitions and may result in violations of the proposed rule and subject the transacting parties to enforcement action. Misrepresentations in the application process may render the license void from the date of issuance and may subject parties to enforcement action. The proposed rule contains provisions authorizing the Department to require applicants for specific licenses to use specific forms and procedures published by the Department. The proposed rule also establishes a process to allow applicants and other parties-in-interest to request reconsideration of the denial of a license based on new facts or changed circumstances.

Under subpart D of the proposed rule, governing restricted transactions, parties may engage in certain otherwise-prohibited transactions if they satisfy the specified security requirements. These provisions operate functionally as a general license to engage in certain prohibited transactions when specific conditions—the security requirements—are met. The Department does not anticipate issuing licenses in the ordinary course to relieve parties from complying with the security requirements for restricted transactions but may do so in unusual or unique circumstances as necessary or appropriate. The Department retains the discretion, however, to issue general or specific licenses that would apply to otherwise restricted transactions.

G. Subpart I—Advisory Opinions

1. Section 202.901—Inquiries Concerning Application of This Part

The proposed rule creates a system for the Attorney General to provide guidance on this part in the form of official guidance or written advisory opinions. The Department may issue official guidance at any time, including to address recurring or novel issues. The Department may also issue guidance in response to specific inquiries received through advisory opinion procedures.

Under the proposed rule, the Department may publish general forms of interpretive guidance, such as Frequently Asked Questions posted online. The Department plans to make any official guidance publicly available to help potentially regulated parties better understand the regulations and the Department's interpretation of the regulations and the Order.

The proposed rule also creates a mechanism for potentially regulated parties to seek opinions about the application of the regulations or the Order to specific transactions. The proposed rule would permit a U.S. person engaging in a transaction potentially regulated by the program to request an interpretation of any provision of this part. Advisory opinions could cover, for example: (1) whether a particular transaction is a prohibited transaction or restricted transaction; and (2) whether a person is a U.S. person, foreign person, or covered person. The proposed rule requires that advisory opinions only be requested regarding actual—not hypothetical—transactions.

The proposed rule sets out procedural and administrative requirements for submitting a request for any advisory opinion, including: (1) that the request be made in writing, *see* § 202.1201; (2) that the request identify all participants in the transaction for which the opinion is being sought (*i.e.,* anonymous requests will not be accepted); and (3) that the request describe the actual, not hypothetical, conduct giving rise to the request for an advisory opinion. Advisory opinions issued in response to a party's request may be published as appropriate. A determination regarding whether an advisory opinion or portions of that opinion are appropriate for publication will include consideration of whether publication complies with applicable laws and regulations (*e.g.,* regarding the protection of confidential business information). In addition, the proposed rule makes clear that each advisory opinion can be relied upon only to the extent that the disclosures made in obtaining the advisory opinion were accurate and complete, and to the extent that those disclosures continue to accurately and completely reflect the circumstances after the advisory opinion is issued. Advisory opinions will reflect the view of the Department of Justice and will not bind any other agency; an advisory opinion does not affect obligations under provisions not specifically discussed in the opinion.

Commenters supported the Department's proposal to provide interpretive guidance to the public. They also requested that the Department publish the decisions for the public's benefit. As stated above, advisory opinions may be published as appropriate in compliance with applicable laws and regulations. One commenter requested that trade associations be allowed to request interpretive guidance on behalf of their members. The proposed rule would allow trade associations to seek guidance on behalf of their members, so long as the guidance sought relates to a specific transaction and identifies the parties to the transaction. Although one commenter requested the ability to seek guidance related to hypothetical transactions, the Department declines to extend the interpretive guidance provision to such transactions to ensure that any such guidance is based on specific, factual circumstances so that it is as helpful to the public as possible. Consequently, the proposed rule adopts the approach described in the ANPRM without change.

H. Subpart J—Due Diligence and Audit Requirements

The Order delegates to the Attorney General, in consultation with relevant agencies, the full extent of the authority granted to the President by IEEPA as may be necessary or appropriate to carry out the purposes of the Order,[217] and it expressly states that the proposed rules will ''address the need for, as appropriate, recordkeeping and reporting of transactions to inform investigative, enforcement, and regulatory efforts.'' [218] The Department of Justice wishes to achieve widespread compliance with the proposed rule, and to gather the information necessary to administer and enforce the program, without unduly burdening U.S. persons or discouraging data transactions that the program is not intended to address.

The Department will encourage U.S. persons subject to the proposed rule to

[217] E.O. 14117 sec. 2(b), 89 FR 15423.

[218] *Id.* sec. 2(c)(viii), 89 FR 15424.

develop, implement, and update compliance programs as appropriate. The compliance program suitable for a particular U.S. person would be based on that person's individualized risk profile and would vary depending on a variety of factors, including the U.S. person's size and sophistication, products and services, customers and counterparties, and geographic locations. The Department may issue guidance on this topic to assist U.S. persons to develop and implement compliance programs. The Department may also consider the adequacy of a compliance program in any enforcement action.

The proposed rule does not impose affirmative due diligence and recordkeeping requirements on every U.S. person engaging in a covered data transaction with a covered person or country of concern. As discussed in part IV.H.1 of this preamble, the proposed rule only imposes affirmative due diligence and recordkeeping requirements as a condition of engaging in a restricted transaction.

Two related commenters expressed concerns that the proposed rule would require U.S. companies to surveil their employees' communications to comply with the prohibitions and restrictions. No changes have been made in response to this comment. The proposed rule does not, on its face or in practice, require surveillance of employees to achieve compliance. Any U.S. person engaging in activities relevant to the proposed rule should take a risk-based approach to their compliance program and ensure that it aligns with their business profile. Like sanctions, export controls, and other national security regulations, any compliance program may include a mix of policies, processes, resources, and technologies to ensure compliance. Important aspects of an effective compliance program may include, for example, senior management support and buy-in (including adequate resources); a routine and ongoing assessment of the business' risk profile to identify potential issues under the regulations that the business is likely to encounter; internal controls informed by that risk assessment, including policies and procedures to identify and address data transactions that may trigger obligations under the regulations, appointing and empowering responsible compliance personnel, integrating these controls into the company's daily operations, and ensuring that employees have adequate training and job-specific knowledge regarding the proposed rule and internal controls; and testing these controls and remediating any weaknesses or gaps.[219] The Department is considering providing separate guidance on implementing effective risk-based compliance programs.

1. Section 202.1001—Due Diligence for Restricted Transactions

As discussed in part IV.H of this preamble, the Order delegates to the Attorney General, in consultation with relevant agencies, the full extent of the authority granted to the President by IEEPA as may be necessary or appropriate to carry out the purposes of the Order.[220] In accordance with that delegation, and adopting the approach contemplated in the ANPRM, the proposed rule imposes and details affirmative due diligence requirements as a condition of engaging in a restricted transaction. The proposed rule imposes know-your-data requirements, which specifically require that U.S. persons engaging in restricted transactions develop and implement data compliance programs with risk-based procedures for verifying data flows, including the types and volumes of data involved in the transactions, the identity of the transaction parties, and the end-use of the data. The Order also requires that the proposed rule address the need for recordkeeping, as appropriate.[221] The proposed rule imposes affirmative recordkeeping requirements as a condition of engaging in a restricted transaction, and requires U.S. persons subject to these affirmative requirements to maintain documentation of their due diligence to assist in inspections and enforcement, and to maintain the results of annual audits that verify their compliance with the security requirements and, where relevant, the license conditions to which the U.S. persons may be subject.

2. Section 202.1002—Audits for Restricted Transactions

Adopting the approach contemplated in the ANPRM, the proposed rule would impose and details an annual audit requirement as a condition of engaging in a restricted transaction to verify and improve compliance with the security requirements.

[219] *See generally* OFAC, U.S. Dep't of Treas., *A Framework for OFAC Compliance Commitments* (May 2, 2019), *https://ofac.treasury.gov/media/16331/download?inline* [*https://perma.cc/6EQY-MD3L*]; Bureau of Indus. & Sec., U.S. Dep't of Com., *Export Compliance Guidelines: The Elements of an Effective Export Compliance Program* (2017), *https://www.bis.doc.gov/index.php/documents/pdfs/1641-ecp/file* [*https://perma.cc/KXT2-TMQ5*].

[220] E.O. 14117 sec. 2(b), 89 FR 15424.

[221] E.O. 14117 sec. 2(c)(viii), 89 FR 15423.

I. Subpart K—Reporting and Recordkeeping Requirements

1. Section 202.1101—Records and Recordkeeping Requirements

Adopting the approach contemplated in the ANPRM, the proposed rule would require any U.S. person engaging in a restricted transaction to keep full and accurate records of each restricted transaction and to keep the records available for examination for at least 10 years after the date of such transaction (the length of the statute of limitations for violations of IEEPA). The proposed rule describes the required records in detail, which include a written policy describing the compliance program, a written policy documenting implementation of the security measures for restricted transactions, the results of any audits to evaluate compliance with the security measures, documentation of the due diligence conducted to verify the data flow involved in any restricted transaction, and other pertinent information regarding each transaction.

2. Section 202.1102—Reports To Be Furnished on Demand

Adopting the approach contemplated in the ANPRM, the proposed rule includes provisions to assist the Department in investigating potential noncompliance with the proposed rules of this program. These include requiring any U.S. person to furnish under oath, from time to time and at any time as may be required by the Attorney General, complete information relative to any covered data transaction subject to a prohibition or restriction.

3. Section 202.1103—Annual Reports

Adopting the approach contemplated in the ANPRM, the proposed rule would require reporting by U.S. persons who engage in certain restricted transactions or, in certain narrow circumstances, to identify attempts to engage in prohibited transactions. Specifically, the proposed rule requires annual reports from U.S. persons engaged in restricted transactions involving cloud-computing services where 25 percent or more of that U.S. person's equity interests are owned (directly or indirectly, through any contract, arrangement, understanding, relationship, or otherwise) by a country of concern or covered person.

The Department may impose similar reporting requirements on U.S. persons engaging in licensed transactions as conditions of specific or general licenses. Those requirements may vary depending on the nature of the licenses, will be set forth in the licenses

themselves, and are not part of the proposed rule.

4. Section 202.1104—Reports on Rejected Prohibited Transactions

Adopting the approach contemplated in the ANPRM, the proposed rule also requires that any U.S. person that has received and affirmatively rejected an offer from another person to engage in a prohibited transaction must submit a report to the Department within 14 business days of rejecting it. These reports will help the Department identify instances in which potential countries of concern or covered persons seek to enter into prohibited transactions with U.S. persons in contravention of the proposed rule, including through evasion. The information submitted by these reports will thus assist the Department in monitoring U.S. persons' compliance with the proposed rule, identifying matters for potential investigation, undertaking enforcement actions, and identifying ways in which to refine the proposed rule in the future.

J. Subpart M—Penalties and Finding of Violation

1. Section 202.1301—Penalties for Violations

Adopting the approach contemplated in the ANPRM, the proposed rule also includes a process for imposing civil monetary penalties similar to those used in other IEEPA-based regimes. *See* 31 CFR part 501, Appendix A; 15 CFR part 764. The proposed rule includes mechanisms for pre-penalty notice, an opportunity to respond, and a final decision. Under the proposed rule, penalties may be based on noncompliance with the proposed rules of this program, material misstatements or omissions in connection with this program, false certifications or submissions pursuant to the proposed rules of this program, or other actions and factors. The proposed rule stipulates that, consistent with due process requirements, the Department of Justice will give the alleged violator any relevant non-classified information that forms the basis of any enforcement action and a meaningful opportunity to respond.

As part of this proposed rulemaking, the Department is adjusting for inflation the civil monetary penalty that can be imposed under IEEPA in accordance with section four of the Federal Civil Penalties Inflation Adjustment Act of 1990 (Pub. L. 101–410, 104 Stat. 890; 28 U.S.C. 2461 note), as amended by the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015 (Pub. L. 114–74, tit. VII, sec. 701, 129 Stat. 584, 599, 28 U.S.C. 2461 note) (''FCPIA Act''), for penalties assessed after the effective date of this proposed part with respect to violations occurring after November 2, 2015.

For consistency with the civil monetary penalties imposed in other, more widely known IEEPA-based regimes administered by the Department of the Treasury's OFAC, the Department of Justice proposes incorporating OFAC's prior annual adjustments to IEEPA's maximum civil monetary penalty as an initial catch-up adjustment applicable to this part. Those adjustments by OFAC occurred on August 1, 2016 (Implementation of the Federal Civil Penalties Inflation Adjustment Act, 81 FR 43070 (July 1, 2016)), February 10, 2017 (Inflation Adjustment of Civil Monetary Penalties, 82 FR 10434 (Feb. 10, 2017)); March 19, 2018 (Inflation Adjustment of Civil Monetary Penalties, 83 FR 11876 (Mar. 19, 2018)); June 14, 2019 (Inflation Adjustment of Civil Monetary Penalties, 84 FR 27714 (June 14, 2019)); April 9, 2020 (Inflation Adjustment of Civil Monetary Penalties, 85 FR 19884 (Apr. 9, 2020)); March 17, 2021 (Inflation Adjustment of Civil Monetary Penalties, 86 FR 14534 (Mar. 17, 2021)); February 9, 2022 (Inflation Adjustment of Civil Monetary Penalties, 87 FR 7369 (Feb. 9, 2022)); January 13, 2023 (Inflation Adjustment of Civil Monetary Penalties, 88 FR 2229 (Jan. 13, 2023)); and January 12, 2024 (Inflation Adjustment of Civil Monetary Penalties, 89 FR 2139 (Jan. 12, 2024)).

The proposed maximum civil monetary penalty for violations of this part after its effective date would therefore be 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.[222] The Department of Justice proposes making annual adjustments to the civil monetary penalty on an annual basis after the effective date of this part consistent with the FCPIA Act.

2. Section 202.1305—Finding of Violation

The proposed rule also provides a process in which the Department might issue a finding of violation where the Department determines that a party has violated the regulations and that an administrative response short of a civil monetary penalty is warranted. As with civil penalties, the proposed rule also provides that, consistent with due process requirements, the Department will give the alleged violator any relevant non-classified information that forms the basis of any finding of violation and a meaningful opportunity to respond.

K. Coordination With Other Regulatory Regimes

The Order requires the Department of Justice to address, as appropriate, coordination with other United States Government entities, such as CFIUS, OFAC, agencies that operate export-control programs, and other entities implementing relevant programs, including those implementing Executive Order 13873; Executive Order 14034 of June 9, 2021 (Protecting Americans' Sensitive Data from Foreign Adversaries); and Executive Order 13913 of April 4, 2020 (Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector).[223] The Department does not currently intend or anticipate that this new program will significantly overlap with existing programs. As explained in the ANPRM, existing programs do not provide prospective, categorical rules to address the national security risks posed by transactions between U.S. persons and countries of concern (or persons subject to their ownership, direction, jurisdiction, or control) that pose an unacceptable risk of providing those countries with access to government-related data or bulk U.S. sensitive personal data.

The Department has identified and considered three potential areas of overlap between this proposed rule and existing regulatory regimes.

First, the Department has considered the potential interaction between this proposed rule's application to investment agreements and CFIUS's authority to review ''covered transactions,'' *see generally* 50 U.S.C. 4565. Some ''investment agreements,'' as defined in the proposed rule, would also be covered transactions or covered real estate transactions subject to CFIUS's jurisdiction. *See* § 202.228; 50 U.S.C. 4565(a)(4). The ANPRM contemplated an approach in which the proposed rule would independently regulate, as a restricted transaction, an investment agreement that is also a covered transaction or covered real estate transaction subject to review by CFIUS unless and until a ''CFIUS action'' occurs in which CFIUS imposes an order or condition or enters into a mitigation agreement to resolve the

[222] *See* 50 U.S.C. 1705(b); Inflation Adjustment of Civil Monetary Penalties, 89 FR 2139 (Jan. 12, 2024).

[223] E.O. 14117, sec. 2(c)(vii), 89 FR 15424.

national security risk arising from the transaction.[224] As explained in the ANPRM, this approach would preserve CFIUS's authority to develop bespoke protections to mitigate risks arising from covered transactions or covered real estate transactions—or recommend that the President prohibit a transaction—where CFIUS concludes that such action is necessary to address the national security risk arising from the transaction. To implement this approach, the ANPRM contemplated an exemption in the proposed rule that would apply categorically for all covered transactions that are subject to CFIUS actions, rather than requiring the Department to issue a specific license for each investment agreement subject to a CFIUS action.

The proposed rule adopts the approach described in the ANPRM and implements that approach by adding a corresponding exemption for any investment agreement that is subject to a ''CFIUS action,'' defining that term, and providing examples. *See* § 202.508. Under the proposed rule, if a CFIUS action occurs with respect to an investment agreement, that investment agreement would become exempt from the proposed rule and would be subject only to CFIUS's authority going forward. The Department, in close coordination with the Department of the Treasury, as chair of CFIUS, would retain enforcement authority with respect to any violations of the proposed rule before the effective date of the CFIUS action. Alternatively, in some instances, CFIUS may not review a particular transaction at all or may conclude its review or assessment of a transaction without taking a CFIUS action. Because CFIUS's authority to mitigate transactions is limited to risks that ''arise[s] as a result'' of the particular transaction, *see* 50 U.S.C. 4565(l)(3)(A)(i), the fact that CFIUS takes no action does not mean that the transaction poses no national security risk. For example, the transaction may implicate pre-existing national security risks that do not arise from the particular transaction CFIUS can review.'' In those scenarios, any obligations under the proposed rule would continue to apply with respect to the transaction. Similarly, if CFIUS requests information from parties about a transaction for which no filing has been submitted to CFIUS under 31 CFR 800.504(b) or 31 CFR 802.501(b), the Department will closely coordinate with the Department of the Treasury with respect to any enforcement action under the proposed rule with respect to that investment agreement. CFIUS may also refer a covered transaction or covered real estate transaction to the President, in which case any obligations under the proposed rule would continue to apply and the Department would closely coordinate with the Department of the Treasury on any enforcement actions under the proposed rule. The same would be true after any Presidential order under 50 U.S.C. 4565(d) following a referral from CFIUS, absent any accompanying CFIUS action. The Department, in consultation with CFIUS member agencies, continues to evaluate alternative approaches, such as regulating investment agreements as restricted transactions regardless of whether they are ''covered transactions'' subject to a CFIUS action. The Department welcomes comments on this potential alternative approach, as well as any other proposed alternatives.

Second, the Department has considered, in consultation with the Federal Trade Commission (''FTC'') and other agencies, the potential interaction between this proposed rule's application to data-brokerage transactions and the Protecting Americans' Data from Foreign Adversaries Act of 2024 (''PADFAA''). *See* Public Law 118–50, div. I 138 Stat. 895, 960 (2024). The PADFAA generally makes it unlawful for a ''data broker to sell'' or ''otherwise make available personally identifiable sensitive data of a United States individual'' to any foreign adversary country or any entity that is controlled by a foreign adversary and authorizes the FTC to bring civil enforcement actions for any violations. The proposed rule would generally prohibit U.S. persons from engaging in covered data transactions involving data brokerage with countries of concern or covered persons.

Following consultation with the FTC, the Department does not believe that it would be appropriate to alter the proposed rule's scope in light of the PADFAA for several reasons. There are significant differences in scope between the PADFAA and the proposed rule. The PADFAA's prohibition applies to entities that meet the statutory definition of ''data broker.'' [225] By contrast, the proposed rule would regulate certain transactions involving ''data brokerage,'' a term that is broader and covers activities that present the national security risk of allowing countries of concern access to sensitive personal data, regardless of the kinds of entities that engage in that activity. In addition, the proposed rule would reach any U.S. persons—including individuals, not just entities—who engage in the regulated categories of activities. Similarly, the PADFAA applies to a narrower category of activities than the proposed rule. Unlike the PADFAA, the proposed rule expressly addresses the re-export or resale of data by third parties and indirect sales through intermediaries. The PADFAA excludes from the definition of ''data broker'' any entity that transmits a U.S. individual's data at that individual's request or direction, whereas the proposed rule would not contain any such exception in light of the national security threat posed even in such instances. In addition, the PADFAA does not provide any mechanisms for affected parties to seek clarification or redress, such as the advisory opinions, general licenses, and specific licenses available to parties under the proposed rule. Similarly, the PADFAA provides general contours for entities and businesses to determine whether a counterparty is ''subject to the direction or control'' of either: (1) a person that is domiciled in, headquartered in, has its principal place of business in, or is organized under the laws of a foreign adversary country; or (2) an entity that is 20-percent or more owned by such a person.[226] The proposed rule provides different criteria for determining whether a person is ''covered'' under the regulatory program, and it contemplates a designation process, which the PADFAA lacks.

Given the PADFAA's structure and the significant differences in scope, the Department declines to alter the proposed rule's scope in light of the PADFAA. The Department and the FTC intend to coordinate closely to ensure that these authorities are exercised in a harmonized way to minimize any conflicting obligations or duplicative enforcement. For example, the Department and the FTC intend to coordinate, as appropriate, on licensing decisions and on any potential enforcement actions under the PADFAA with respect to activities that may be authorized, exempt, or licensed under the proposed rule. Thus, the proposed rule adopts the approach described in the ANPRM without change.

Third, the Department has considered the potential interaction between this proposed rule's application to vendor agreements and any actions taken by the Secretary of Commerce under Executive Orders 13873 and 14034. Some vendor agreements, as defined in this proposed

[224] 89 FR 15798–99.

[225] Protecting Americans' Data from Foreign Adversaries Act of 2024, Pub. L. 118–50, div. I, sec. 2(c)(3) 138 Stat. 895, 960 (2024).

[226] *Id.* at sec. 2(c)(2).

rule, could also be the subject of an action by the Secretary of Commerce regarding an information and communications technology and services (''ICTS'') transaction that involves ICTS that is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary and presents the types of unacceptable national security risks described in Executive Orders 13873 and 14034. Even so, the Department does not believe that it would be appropriate to alter the scope of this proposed rule for several reasons. While these two authorities could potentially address some of the same national security risks related to vendor agreements, they would do so in different ways and by focusing on different vectors of risk. Executive Order 14117 and this proposed rule seek to address this risk by addressing transactions involving the export of U.S. sensitive personal data, such as restricting a U.S. person's ability to enter into a vendor agreement that grants access to government-related data or bulk U.S. sensitive personal data to a country of concern or covered person. Executive Orders 13873 and 14034, on the other hand, seek to address transactions involving the acquisition, import, or use, among other actions, of technology or services developed or otherwise sourced from a foreign adversary by U.S. persons or in the United States. For that reason, the ICTS authority addresses a broader range of potential national security risks than access to Americans' bulk sensitive personal data.

In addition, this proposed rule (through the incorporation by reference of the CISA security requirements for restricted transactions, including vendor agreements) creates a floor for the security of all government-related data or Americans' bulk U.S. sensitive personal data involved in a restricted transaction. Only by complying with these requirements (or operating under an applicable license) could a U.S. person engage in a proposed restricted transaction. Executive Order 13873 and its implementing regulations do not establish a baseline set of mitigation measures to protect this data across all of types of vendors that could be subject to prohibition or restriction. Rather, the Department of Commerce will exercise that authority by taking an action with respect to transactions involving a specific vendor [227] or proposing regulation of a sector-specific set of ICTS.[228] Nothing in this proposed rule would prevent the Department of Commerce from exercising its ICTS authorities to take vendor-specific actions or promulgate sector-specific rules. At this time, any overlap between these two authorities is hypothetical, and the Department does not believe that there will be any substantial impact. The Department is, however, considering approaches to address any potential overlap that might arise between the requirements of this proposed rule and any ICTS actions undertaken by the Department of Commerce, whether through an understanding between the Department of Commerce and Department of Justice or a more formal licensing process that could apply where the Department of Commerce has taken action under its ICTS authorities. The Department welcomes comments on the identified approaches, or any others, to address any potential overlap that might arise.

L. Severability

The Department intends for the provisions of this proposed rule to be severable from each other. In short, if a court holds that any provision in a final 28 CFR part 202 is invalid or unenforceable, the Department intends that the remaining provisions of a final 28 CFR part 202, as relevant, would continue in effect to the greatest extent possible. In addition, if a court holds that any such provision is invalid or unenforceable as to a particular person or circumstance, the Department intends that the provision would remain in effect as to any other person or circumstance. Depending on the circumstances and the scope of the court's order, remaining provisions of a final rule likely could continue to function sensibly independent of any provision or application held invalid or unenforceable. For example, the prohibitions and restrictions related to transactions involving access to personal health data could continue to apply even if a court finds that the restrictions or prohibitions on transactions involving access to biometric data are invalid. Similarly, the proposed rule could be applied with respect to North Korea even if a court finds its application with respect to Russia is invalid.

V. Analysis for Proposed Bulk Thresholds

The Department of Justice proposes volume-based thresholds for each category of sensitive personal data and for combined datasets. The bulk thresholds are based on a risk-based assessment that accounts for the characteristics of datasets that affect the data's vulnerability to exploitation by countries of concern and that affect the consequences of exploitation. In conducting this assessment, the Department considered numerous ways that a country of concern might exploit each category of sensitive personal data. In general, bulk U.S. sensitive personal data is useful for deriving additional information about individuals or subpopulations, such as demography, geography, and interests, that can be used to identify vulnerabilities.[229] The advertising industry has long recognized that such data is useful for predicting and influencing behavior.[230] Influencing behavior is similarly at the root of intelligence recruitment.[231] The Department assessed how a foreign intelligence service might use bulk U.S. sensitive personal data as part of the agent recruitment cycle—a ''systematic method for finding agents who will meet national intelligence information needs''—among other potential malign uses.[232] While the categories of sensitive personal data may have a variety of applications for foreign intelligence services or foreign governments, they may be especially useful to parts of the first three steps of agent recruitment:

- ''spotting (or identifying) individuals who can meet intelligence needs'';
- ''assessing whether the spotted individuals have the placement and access to provide desired information''; and

[227] *See* Kaspersky Lab, Inc., 89 FR 52435 n.13; Maggs Report, *supra* note 187.

[228] *See* Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 89 FR 15066 (Mar. 1, 2024) (to be codified at 15 CFR pt. 7), *https://www.federalregister.gov/documents/2024/03/01/2024-04382/securing-the-information-and-communications-technology-and-services-supply-chain-connected-vehicles* [*https://perma.cc/PV7Y-998V*].

[229] *What Is Targeted Advertising, and How Does It Work?,* RTB House (May 13, 2024), *https://blog.rtbhouse.com/what-is-targeted-advertising-and-how-does-it-work/* [*https://perma.cc/EQ5Q-M6KD*].

[230] *See The Role of Data in the Targeted Advertising Industry,* New Am., *https://www.newamerica.org/oti/reports/special-delivery/the-role-of-data-in-the-targeted-advertising-industry/* [*https://perma.cc/LMX7-B93Q*]; Ben Collier, *Targeted Social Media Ads Are Influencing Our Behaviour—and the Government Uses Them Too,* Conversation (Feb. 27, 2024), *https://theconversation.com/targeted-social-media-ads-are-influencing-our-behaviour-and-the-government-uses-them-too-223576* [*https://perma.cc/YGA8-YKF9*].

[231] *See id.;* Randy Burkett, *An Alternative Framework for Agent Recruitment: From MICE to RASCLS,* 57 Stud. Intel. 7, 13 (2013), *https://www.cia.gov/resources/csi/static/9ccc45dc156271d11769e5205ec49c29/Alt-Framework-Agent-Recruitment-1.pdf* [*https://perma.cc/9GQU-UTET*]; Collier, *supra* note 230.

[232] Burkett, *supra* note 231, at 13.

• ''developing a relationship with the individual to . . . explore whether they will be responsive to . . . tasking for intelligence information.'' [233]

The Department's subject-matter experts identified seven characteristics relevant to the exploitability and national security harm posed by any particular type of data: purpose (*i.e.,* how the data can be used), changeability (*i.e.,* how easy it would be for an individual to deliberately change or falsify the data in question), control (*i.e.,* who tracks and manages the data), availability (*i.e.,* how easily the data can be obtained), volume (*i.e.,* the number of data points in a dataset), velocity (*i.e.,* how quickly the dataset evolves), and quality (*i.e.,* how much processing is required to use the data). These characteristics help describe the national security risk of each type of sensitive personal data by providing a methodology for analyzing their value to an adversary. For example, availability and control focuses on the ease with which an adversary may be able to acquire this data using licit or illicit means. Quality and changeability examine the ease and speed with which an adversary can use the data. Volume, velocity, and purpose are other important attributes of these datasets that focus on how valuable a particular data may be to an adversary and how long it is likely to remain valuable.

Using this framework of characteristics, the Department evaluated the relative sensitivity of each of the seven categories of bulk U.S. sensitive personal data and ranked them based on their potential value to enable foreign governments and foreign intelligence services engaged in agent recruitment to: (1) identify or spot individuals within bulk datasets for intelligence needs; (2) group individuals into specific categories to assess their value for intelligence purposes; and (3) characterize the behaviors and vulnerabilities of individuals to identify ways to develop and exploit relationships. The Department then considered how close in sensitivity each category was to the other, grouped them into tiers of similar sensitivity (resulting in four tiers), and then set proposed numerical thresholds for each tier.

To conduct the analysis, the Department considered use cases from each category of bulk U.S. sensitive personal data based on widely available information about commercial practices around data,[234] news reports of past incidents involving data with national security implications,[235] and a survey of covered transactions reviewed by CFIUS that implicated sensitive personal data. The Department also considered how future changes in technology could affect the utility and value of each category of data.[236]

A. Analysis of Sensitivity of Each Category of Sensitive Personal Data

1. Human Genomic Data

The Department of Justice assesses that human genomic data is the most sensitive category of sensitive personal data. To conduct the analysis, the Department considered human genetic testing data, which sequences only specific portions of the human genome for a specific purpose (*e.g.,* identifying ancestry, diagnosing a specific disease); and sequencing of a complete human genome, a still-emerging capability with a wide variety of potential applications.[237] Based on the multiple characteristics that were considered of high sensitivity, and especially noting that the velocity of this data has very high sensitivity, human genomic data is highly sensitive:

• *Purpose:* High sensitivity. Human genomic data has unique purposes among the categories of bulk U.S. sensitive personal data. It is not only useful for identifying traits such as health, emotional stability, mental capacity, appearance, and physical abilities that might be useful in intelligence recruitment; countries of concern may also use this data to develop military capabilities such as bioweapons.[238] Because human genomic data includes the unique genetic code of an individual, it is exceptionally useful in identifying individuals.[239] For example, an adversary with access to an individual's genomic data may be able to predict physical features, such as eye, hair, and skin color, and vocal and facial characteristics.[240] As technology develops further, analysts may also be able to use such genomic data to determine an individual's propensity toward certain behaviors, such as aggression or risky activities.[241] Finally, foreign adversaries could potentially use human genomic data to conduct or support surveillance, oppression, extortion, and influence operations; and could potentially use this data to inform biological weapons development.[242]

• *Changeability:* High sensitivity. Human genomic data is difficult to deliberately alter. While certain technologies, such as Clustered Regularly Interspaced Short Palindromic Repeats (''CRISPR''), can alter or edit the human genome in extremely targeted, localized ways, larger-scale alterations remain technologically impossible.[243] As a result, human genomic data is largely immutable over an individual's lifetime.

• *Control:* High sensitivity. Corporate entities such as healthcare laboratories usually process and control human

---

[233] *Id.*

[234] *See, e.g.,* Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It),* Bus. News Daily (Oct. 20, 2023), *https://www.businessnewsdaily.com/10625-businesses-collecting-data.html* [*https://perma.cc/944W-ZC4M*].

[235] *See, e.g.,* Hsu, *supra* note 43; Garrett M. Graff, *China's Hacking Spree Will Have a Decades-Long Fallout,* Wired (Feb. 11, 2020), *https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/* [*https://perma.cc/48WK-M9AM*]; Press Release, U.S. Dep't of Just., *Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting Over 78 Million People* (May 9, 2019), *https://www.justice.gov/opa/pr/member-sophisticated-china-based-hacking-group-indicted-series-computer-intrusions-including* [*https://perma.cc/84YH-CVA5*].

[236] *See, e.g.,* Steve Van Kuiken, *Tech at the Edge: Trends Reshaping the Future of IT and Business,* McKinsey Digital (Oct. 21, 2022), *https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-at-the-edge-trends-reshaping-the-future-of-it-and-business* [*https://perma.cc/HW2S-N464*]; Adam D. Nahari & Dimitris Bertsimas, *External Data and AI Are Making Each Other More Valuable,* Harv. Bus. Rev. (Feb. 26, 2024), *https://hbr.org/2024/02/external-data-and-ai-are-making-each-other-more-valuable* [*https://perma.cc/2ZAS-8VBB*].

[237] Luca Bonomi et al., *Privacy Challenges and Research Opportunities for Genomic Data Sharing,* 52 Nature Genetics 646 (2020), *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7761157/* [*https://perma.cc/2J8T-BLLF*].

[238] Ken Dilanian, *Congress Wants to Ban China's Largest Genomics Firm from Doing Business in the U.S. Here's Why,* NBC News (Jan. 25, 2024), *https://www.nbcnews.com/politics/nationalsecurity/congress-wants-ban-china-genomics-firm-bgi-from-us-rcna135698* [*https://perma.cc/T2Y2-R7RZ*]; Ron Pulivarti et al., Nat'l Inst. of Standards & Tech., NIST IR 8432, *Cybersecurity of Genomic Data* 9 (2023), *https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8432.pdf* [*https://perma.cc/5D3G-BEEZ*].

[239] Bonomi et al., *supra* note 237.

[240] Christopher Lippert et al., *Identification of Individuals by Trait Prediction Using Whole-Genome Sequencing Data,* 114 PNAS 10166 (Sept. 5, 2017), *https://www.pnas.org/doi/full/10.1073/pnas.1711125114* [*https://perma.cc/CM4L-GPE4*].

[241] J.C. Barnes et al., *The Propensity for Aggressive Behavior and Lifetime Incarceration Risk: A Test for Gene-Environment Interaction (G x E) Using Whole-Genome Data,* 49 Aggr. & Violent Behav. (Nov.–Dec. 2019), *https://www.sciencedirect.com/science/article/abs/pii/S1359178919300631* [*https://perma.cc/3GVF-MPKF*]; Heather Buschman, *Large Study Identifies Genetic Variants Linked to Risk Tolerance and Risky Behaviors,* UC San Diego Health (Jan. 2019), *https://health.ucsd.edu/news/press-releases/2019-01-14-large-study-identifies-genetic-variants-linked-to-risk-tolerance-risky-behaviors/* [*https://perma.cc/FMV2-GKYE*].

[242] Pulivarti et al., *supra* note 238, at 9.

[243] *What Are Genome Editing and CRISPR-Cas9?,* MedlinePlus (updated Mar. 22, 2022), *https://medlineplus.gov/genetics/understanding/genomicresearch/genomeediting/* [*https://perma.cc/42K9-765F*].

genomic data.[244] Because human genomic data is tied to an individual at a biological level, it is basically immutable. Additionally, biological residue such as saliva, blood, and hair can contain human genomic data, and this residue is difficult for an individual to completely control.[245]

- *Availability:* High sensitivity. Bulk human genomic data is difficult to obtain in the commercial marketplace, as it remains an emerging capability. For example, the crucial technologies that formed the foundation for scaled commercial applications of genomic sequencing are still less than 20 years old.[246] In addition, medical systems tightly control access to and distribution of this information through privacy regulations and general scientific ethics.[247] Because this data is currently hard to acquire but has myriad potential applications, it is highly valued.
- *Volume:* Varied sensitivity. A complete human nuclear genome contains about 3.2 billion base pairs, with each base pair representing a unique data point.[248] This human genome can be divided into codons of three base pairs each, each of which codes for a unique amino acid.[249] This human genome can also be divided into tens of thousands of genes, each of which code for the production of specific proteins and other cellular activity and each of which can have multiple variants.[250] Data sets containing human genomic data will be of different sizes—for example, a data set including the complete genome of an individual will be much larger than the data set just identifying specific genes present that may affect the chances of a specific cancer. A larger data set is more sensitive. Thus, the volume sensitivity of genomic information may vary because the datasets containing human genomic data are likely to vary widely in size.
- *Velocity:* Very high sensitivity. Human genomic data remains largely stable over an individual's lifetime, and while the ability to interpret that data may evolve over time, the underlying information will not change.[251] Furthermore, the value of human genomic data will likely increase significantly in the future as technology develops.[252] It requires protection now to prevent future exploitation.[253]
- *Quality:* Varied sensitivity. Processing a single sample of human genomic data can take as long as 48 hours. As a result, computing power continues to limit analysts' ability to use fully sequenced but unevaluated human genomic data.[254] However, analysts will be increasingly able to take advantage of public databases and open-source tools to evaluate sequenced and analyzed data, reducing the computational power required to evaluate such processed datasets.[255]

2. Biometric Identifiers

The Department of Justice assesses that biometric identifiers are the second most sensitive category of sensitive personal data. To conduct the analysis, the Department considered physical biometrics measurements (*e.g.,* eye patterns, fingerprints, facial features) as well as behavioral biometrics measurements (*e.g.,* gait, keystroke recognition, signature).[256] Biometric data is moderately to highly sensitive overall based primarily on the purpose, changeability, and control characteristics below:

- *Purpose:* High sensitivity. Biometric data is specifically intended to identify specific individuals based on distinguishing biological or behavioral characteristics.[257] In addition, analysts can identify certain categorizing characteristics from this data—for example, inferring gender from facial features.[258] Finally, biometric information can be used to authenticate users, either alone or as part of a multi-factor authentication protocol. Fingerprints, voiceprints, and facial scans provide useful reference points for identifying individuals for intelligence recruitment, espionage, and influence based on their patterns of life. Searches through video footage, police records, and intelligence databases using biometrics could provide points of leverage for coercion, blackmail, and influence.
- *Changeability:* Moderate-to-high sensitivity. Biometric data is generally difficult to deliberately change or falsify because it is linked to the physical characteristics of an individual. However, it can evolve as individuals age or be altered through activities such as limb loss or amputation, long-term manual labor, or physical retraining.[259]
- *Control:* Moderate-to-high sensitivity. Physical biometric information is largely beyond the ability of an individual to control or conceal. If an individual's fingerprint or other

[244] Bonomi et al., *supra* note 237, at Table 2; *Genomic & Infrastructure Services,* Quest Diagnostics, *https://www.questdiagnostics.com/business-solutions/life-sciences/biotech/genomic-infrastructure-services* [*https://perma.cc/WD2E-2YXA*].

[245] Am. Bar Ass'n, *ABA Standards for Criminal Justice: DNA Evidence* at 25 (3d ed. 2007), *https://www.americanbar.org/content/dam/aba/publications/criminal_justice_standards/dna_evidence.pdf* [*https://perma.cc/3CSA-Q6J9*]; Alexia Ramirez, *Police Need a Warrant to Collect DNA We Inevitably Leave Behind,* ACLU (Mar. 10, 2020), *https://www.aclu.org/news/privacy-technology/police-need-a-warrant-to-collect-dna-we-inevitably-leave-behind* [*https://perma.cc/9MGJ-LDZP*].

[246] Joseph Wilson, *Sequencing—The Next Generation,* Nature (Feb. 10, 2021), *https://www.nature.com/articles/d42859-020-00103-7* [*https://perma.cc/PY2Q-GKNY*].

[247] *Privacy in Genomics,* Nat'l Hum. Genome Rsch Inst. (Feb. 6, 2024), *https://www.genome.gov/about-genomics/policy-issues/Privacy* [*https://perma.cc/2YU5-GBRZ*].

[248] Terence A. Brown, *The Human Genome, in* Genomes (2d ed. 2002), *https://www.ncbi.nlm.nih.gov/books/NBK21134/* [*https://perma.cc/Q9EW-FB7E*].

[249] *Codon,* Nat'l Cancer Inst., *https://www.cancer.gov/publications/dictionaries/genetics-dictionary/def/codon* [*https://perma.cc/GDB6-T32U*].

[250] *See* Steven L. Salzberg, *Open Questions: How Many Genes Do We Have?,* 16 BMC Biology (Aug. 20, 2018), *https://bmcbiol.biomedcentral.com/articles/10.1186/s12915-018-0564-x* [*https://perma.cc/89MV-J6HU*].

[251] Kate Lyle et al., *Immortal Data: A Qualitative Exploration of Patients' Understandings of Genomic Data,* 31 Eur. J. Hum. Genetics 681 (Mar. 31, 2023), *https://doi.org/10.1038/s41431-023-01325-9* [*https://perma.cc/V6BM-NEE8*].

[252] *Genomic Data Science,* Nat'l Hum. Genome Rsch Inst. (Apr. 5, 2022), *https://www.genome.gov/about-genomics/fact-sheets/Genomic-Data-Science* [*https://perma.cc/8YD2-MQZJ*]; Nat'l Counterintel. & Sec. Ctr., *supra* note 83.

[253] Pulivarti et al., *supra* note 238, at 7–10.

[254] *See* Nathan Eddy, *High-Performance Computing Breaks the Genomics Bottleneck,* HealthTech (Feb. 13, 2023), *https://healthtechmagazine.net/article/2023/02/high-performance-computing-breaks-genomics-bottleneck* [*https://perma.cc/LCD5-X3K2*].

[255] *See, e.g., Genome,* Nat'l Libr. Med., *https://www.ncbi.nlm.nih.gov/genome/* [*https://perma.cc/XEV9-FRYH*].

[256] Sterling Miller, *The Basics, Usage, and Privacy Concerns of Biometric Data,* Thomsons Reuters (July 20, 2022), *https://legal.thomsonreuters.com/en/insights/articles/the-basics-usage-and-privacy-concerns-of-biometric-data* [*https://perma.cc/92HR-4YMX*]; *Types of Biometrics,* Biometrics Inst., *https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/* [*https://perma.cc/W7FD-5P6B*].

[257] Int'l Org. for Standardization, ISO/IEC TR 24741:2018, *Information Technology—Biometrics—Overview and Application* (2018), *https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:24741:ed-2:v1:en* [*https://perma.cc/P3RB-56RM*]; *see What Is Biometrics?,* Biometrics Inst., *https://www.biometricsinstitute.org/what-is-biometrics/* [*https://perma.cc/2APY-5WBM*].

[258] D. Gowtami Annapurna et al., *Gender Identification from Facial Features,* 15 Int'l J. Innovations Eng'g & Tech. 5 (2020), *https://ijiet.com/wp-content/uploads/2020/03/21.pdf* [*https://perma.cc/9M69-GXZ8*].

[259] *See, e.g.,* Jesse M. Charlton et al., *Learning Gait Modifications for Musculoskeletal Rehabilitation: Applying Motor Learning Principles to Improve Research and Clinical Implementation,* 101 Physical Therapy, Feb. 2021, at 2, *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7899063/* [*https://perma.cc/JJ9W-CKDA*]; Javier Galbally et al., *A Study of Age and Ageing in Fingerprint Biometrics,* 14 IEEE Transactions on Info. Forensics & Sec. 1351 (2019), *https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8509614* [*https://perma.cc/FK88-THWY*]; *Physiological and Behavioural Biometrics,* Biometrics Inst., *https://www.biometricsinstitute.org/physiological-and-behavioural-biometrics/* [*https://perma.cc/8QE4-LW74*].

physiological biometric measurement is compromised, it can be impossible to change.[260] Additionally, covert or passive measures such as surveillance cameras or latent fingerprints can capture biometric data without the targeted individual's knowledge.[261] However, certain types of behavioral biometric information, such as gait and voice, may be possible to change, though it may be difficult.

- *Availability:* Moderate sensitivity. Certain types of biometric data could be widely available in certain records, such as facial features derived from photographs on the internet.[262] Others, such as gait, are not widely available. Reliable bulk biometric databases remain difficult enough to assemble that they are seen as important national security assets.[263]
- *Volume:* Varied sensitivity. Video surveillance footage, which could be used to derive biometric information from tens or hundreds of individuals walking by the camera, collects up to 30 frames of potentially high-definition photo images per second.[264] In contrast, a single human face can be represented by approximately 80 distinct nodal points, each of which could be represented as a single number.[265]
- *Velocity:* Moderate sensitivity. Certain types of biometric information can change, for example as individuals age or change weight.[266] However, because biometrics are physical, many will remain substantially the same over a person's lifetime. For example, fingerprints are constant over a lifetime, and iris patterns remain largely stable even as children grow.[267]
- *Quality:* Varied sensitivity. Factors including the quality of sensors and environmental conditions can affect the reliability of readings stored in databases.[268] The complex nature of most biometric data systems means data quality can be further affected by obscured or degraded characteristics, subject behavior, data collection, compression and sampling efforts, feature extraction issues, matching errors, and administrative and database problems.[269] As a result, the value of a bulk biometric data source to an analyst will depend on the quality of the underlying dataset.

3. Precise Geolocation Data

The Department of Justice assesses that precise geolocation data is the third most sensitive category of sensitive personal data. To conduct the analysis, the Department considered geolocation measurements obtained by a variety of means, including Global Positioning Systems (''GPS''), cell tower proximity, Wi-Fi networks, Bluetooth signals, and IP geolocation.[270] It considered use cases where sets of geolocation points were linked to a specific device and included timestamps; were linked to a specific device but did not include timestamps; and were not linked to either specific devices or timestamps but instead represented an aggregate picture of where individuals were taking devices. In many—but not all—instances across these use cases, precise geolocation data is moderately to highly sensitive based primarily on the purpose, changeability, volume, and quality characteristics below:

- *Purpose:* High sensitivity. Analysts can use geolocation data to derive detailed information about patterns of life, as well as other types of sensitive personal data such as home address and place of work.[271] They may use it to identify influential individuals for blackmail and coercion, physically map and target sensitive sites and high-risk personnel, create near-real-time situational awareness, and target offensive cyber operations.[272] They may also use it to identify a specific person, such as who goes to a residence, as well as large numbers of people, such as everyone who goes to the Pentagon.[273]
- *Changeability:* Moderate sensitivity. Geolocation data is technically collected (*i.e.,* derived from signals and electronic devices). As a result, individuals can spoof or alter this data with some effort. One common way to affect the apparent location of a device is through a Virtual Private Network (''VPN''), which can affect the apparent location of a device based on its IP address, while connected applications that can spoof a GPS location on a cellphone are readily available online.[274] More complicated spoofing techniques require transmission of a false radio signal to override a legitimate GPS signal.[275]
- *Control:* Moderate sensitivity. Precise geolocation data is collected from electronic devices, which an individual can typically leave behind or be separated from. However, these devices usually collect geolocation data in the background, often beyond the control or visibility of the individual, using software services built into device operating systems.[276] These sensors are

[260] *See* Off. of the Victorian Info. Comm'r, *Biometrics and Privacy—Issues and Challenges* (July 2019), *https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges/* [*https://perma.cc/ME8R-XWJU*]; *Is Biometric Information Protected by Privacy Laws?,* Bloomberg L. (June 20, 2024), *https://pro.bloomberglaw.com/insights/privacy/biometric-data-privacy-laws/* [*https://perma.cc/56EZ-69HK*].

[261] *Id.*

[262] Katherine Tangalakis-Lippert, *Clearview AI Scraped 30 Billion Images from Facebook and Other Social Media Sites and Gave Them to Cops: It Puts Everyone into a 'Perpetual Police Line-Up',* Bus. Insider (Apr. 2, 2023), *https://www.businessinsider.com/clearview-scraped-30-billion-images-facebook-police-facial-recogntion-database-2023-4* [*https://perma.cc/6LZG-NBUT*].

[263] Kelsey Atherton, *The Enduring Risks Posed by Biometric Identification Systems,* Brookings Inst. (Feb. 9, 2022), *https://www.brookings.edu/articles/the-enduring-risks-posed-by-biometric-identification-systems/* [*https://perma.cc/65DW-832R*].

[264] Optiview, *A Practical Guide to CCTV Video Resolutions, https://optiviewusa.com/cctv-video-resolutions/* [*https://perma.cc/K24Y-MJA5*].

[265] Chris De Silva et al., NEC Corp., *It's All About the Face: Face Recognition* (2013), *https://www.nec.com/en/global/solutions/safety/pdf/NEC-FR_white-paper.pdf* [*https://perma.cc/P5PJ-8LQ2*].

[266] Joel R. McConvey, *How Aging, Injury and Capture Impact the Challenge of Change in Biometric Identifiers,* Biometric Update (Dec. 25, 2023), *https://www.biometricupdate.com/202312/how-aging-injury-and-capture-impact-the-challenge-of-change-in-biometric-identifiers* [*https://perma.cc/285T-5L2E*].

[267] Justin Lee, *New Research Proves that Fingerprint Accuracy Remains Unchanged Over Time,* Biometric Update (June 30, 2015), *https://www.biometricupdate.com/201506/new-research-proves-that-fingerprint-accuracy-remains-unchanged-over-time* [*https://perma.cc/C95U-DSSS*]; Priyanka Das et al., *Iris Recognition Performance in Children: A Longitudinal Study,* 3 IEEE Transactions on Biometrics, Behav. & Identity Sci. 138 (Jan. 13, 2021), *https://ieeexplore.ieee.org/document/9321488* [*https://perma.cc/X2KJ-G4EE*].

[268] Off. of the Victorian Info. Comm'r, *supra* note 260.

[269] Austin Hicklin & Rajiv Khanna, Mitretek Sys., *The Role of Data Quality in Biometric Systems* (Feb. 9, 2006), *https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=a892c6e2cf2fdd94bab672a987940f2bb6996119* [*https://perma.cc/4YWP-KDWH*].

[270] Paige M. Boshell, *The Power of Place: Geolocation Tracking and Privacy,* Bus. L. Today (Mar. 25, 2019), *https://businesslawtoday.org/2019/03/power-place-geolocation-tracking-privacy/* [*https://perma.cc/MWB2-7BWN*]; Daniel Ionescu, *Geolocation 101: How It Works, the Apps, and Your Privacy,* PCWorld (Mar. 29, 2010), *https://www.pcworld.com/article/511772/geolo.html* [*https://perma.cc/C28D-XYXU*].

[271] Hsu, *supra* note 43.

[272] Hazelrig, *supra* note 4.

[273] Alex Hern, *Fitness Tracking App Strava Gives Away Location of Secret US Army Bases,* The Guardian (Jan. 28, 2018), *https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases* [*https://perma.cc/J7N3-BHKU*]; Hsu, *supra* note 43.

[274] *See, e.g.,* Shweta, *What a VPN Hides (And What It Doesn't),* Forbes Advisor (June 5, 2024), *https://www.forbes.com/advisor/business/software/what-does-vpn-hide/* [*https://perma.cc/MF23-SYK7*]; Tim Fisher, *How to Fake a GPS Location on Your Phone,* Lifewire (June 18, 2024), *https://www.lifewire.com/fake-gps-location-4165524* [*https://perma.cc/ZB8S-X3ZB*].

[275] *What Is GPS Spoofing and How Do You Defend Against It?,* Okta (Aug. 16, 2023), *https://www.okta.com/identity-101/gps-spoofing/* [*https://perma.cc/ZM7K-4349*].

[276] *See, e.g., Build Location-Aware Apps,* Google for Developers (July 1, 2024), *https://developer.android.com/develop/sensors-and-location/location*[*https://perma.cc/LVM6-TZGK*].

present in an increasing number of devices, including phones, cars, and smartwatches.[277]

• *Availability:* Moderate sensitivity. Commercial companies collect geolocation data in large volumes and consider it valuable for identifying consumers and evaluating their behavior.[278] It is subject to increasing regulatory protection, with laws passed in California and Virginia to regulate precise geolocation data, and Massachusetts considering a law that would ban the sale of user location data as of the date of the proposed rule.[279] These restrictions make the date more sensitive because it is less generally available.

• *Volume*: High sensitivity. Technically, geolocation is often a combination of latitude and longitude, along with related fields such as timestamps, accuracy measurements, device identifiers, and IP addresses.[280] This string of information requires relatively little space to store and is simple, and geolocation information is often collected in very large quantities to be meaningful for commercial or research purposes at scale. For example, one provider of geolocation data advertised a dataset covering 1 year with 214 million daily data points, suggesting the relatively small amount of information contained in each data point.[281] In general, geolocation data is sold in many differently sized sets and different ways, ranging from small, precisely targeted geofenced areas using ads to global datasets containing records on billions of devices.[282]

• *Velocity:* Low sensitivity. Commercially available geolocation datasets typically offer 1 to 5 years of data.[283] This indicates a relatively limited lifespan and may vary. Compared to other types of data under consideration, this data is less valuable and useful over long time periods due to other factors such as volume.

• *Quality:* Moderate sensitivity. Analysts can purchase geolocation data in a variety of formats, including real-time and historical data, over a variety of geographic locations.[284] Analysts can determine valuable information about patterns of life from this information.[285] However, this data is generally provided as raw, unprocessed ''pings,'' which require machine analysis to derive useful insights.

4. Personal Health Data

The Department of Justice assesses that personal health data is the fourth most sensitive category of sensitive personal data. In conducting the analysis, the Department considered personal health records as well as claims and billing information. Unlike the three categories discussed in parts V.A.1, V.A.2, and V.A.3 of this preamble, personal health data contains a much more heterogeneous set of data, with sensitivity varying across the evaluated characteristics. Based primarily on the purpose, control, and availability characteristics described below, the Department assesses personal health data to be moderately sensitive overall:

• *Purpose:* Moderate sensitivity. Personal health records contain a variety of information, including information on medical history, medications, treatments, tests, immunizations, implanted devices, and associated data.[286] They may also contain financial information (where related to billing), and covered personal identifiers.[287] As a result, analysts could use them for a variety of identifying, characterizing, and categorizing activities, including identifying vulnerabilities in an individual's background that could be leveraged to coerce that individual into recruitment by a foreign intelligence service. For example, healthcare records can reveal healthcare providers and embarrassing or expensive medical conditions that help our adversaries target individuals and groups for intelligence recruitment, espionage, and influence. Severe injuries, chronic medical conditions, and mental health information provide points of leverage for coercion, blackmail, and influence. In extreme circumstances, countries of concern could even exploit information gathered from personal health records to target individuals using certain medical devices or taking certain prescriptions.[288]

• *Changeability:* Moderate sensitivity. Many medical records contain objective information, such as laboratory test results and physical measurements. They also contain information that an individual could falsify by providing an inaccurate medical history, describing false symptoms, and hiding certain behaviors or habits to avoid negative consequences, get access to medication or insurance, or for simple emotional reasons such as guilt or shame.[289]

• *Control:* Moderate sensitivity. Personal health records are often based on information provided by an individual and subject to strict privacy laws that help ensure individual control of this data.[290] As a result, this data may not be available without an individual's permission. However, it is typically maintained by third parties, such as doctors, hospitals, and insurance systems, placing it in record systems outside an individual's direct control.[291]

---

[277] Rob Gabriele, *170 Million Americans Own GPS Tracking Devices; Market to Grow Over Next Six Months,* SafeHome.org (July 15, 2024), *https://www.safehome.org/gps-industry-outlook-statistics/* [*https://perma.cc/C3ZY-2WCA*]; Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, *supra* note 228.

[278] Robert Archacki et al., *Unlocking Value with Location Intelligence,* Bos. Consulting Grp. (Feb. 4, 2021), *https://www.bcg.com/publications/2021/leveraging-location-intelligence-across-industries* [*https://perma.cc/XM6A-NQRG*].

[279] BCLP, *Precise Geolocation: Recent Trends and Enforcement,* JD Supra (Mar. 30, 2023), *https://www.jdsupra.com/legalnews/precise-geolocation-recent-trends-and-8834493/* [*https://perma.cc/4YMR-J8NE*]; Will Shanklin, *Massachusetts Weighs Outright Ban on Selling User Location Data,* Engadget (July 10, 2023), *https://www.engadget.com/massachusetts-weighs-outright-ban-on-selling-user-location-data-191637974.html* [*https://perma.cc/X43U-Q35P*].

[280] *Geolocation Data 101: A Guide to Powerful Place-Based Insights,* Zartico, *https://www.zartico.com/blog/guide-to-using-geolocation-data#where-does-geolocation-come-from* [*https://perma.cc/M6SG-5PRF*]; *see* Amended Complaint ¶¶ 27–28, *Fed. Trade Comm'n* v. *Kochava, Inc.,* No. 22–cv–00377 (D. Idaho 2023), ECF No. 26, *https://www.ftc.gov/system/files/ftc_gov/pdf/26AmendedComplaint%28unsealed%29.pdf* [*https://perma.cc/4KWL-ZEJE*].

[281] *Factori Products,* Datarade, *https://datarade.ai/data-providers/lifesight/data-products* [*https://perma.cc/3XEP-9BVH*].

[282] *See* Jon Keegan & Alfred Ng, *There's a Multibillion-Dollar Market for Your Phone's Location Data,* Markup (Sept. 30, 2021), *https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data* [*https://perma.cc/3TUV-HHGV*].

[283] *See, e.g., What Is Mobile Location Data? Definition, Uses, Datasets, & Providers,* Datarade (Sept. 23, 2024), *https://datarade.ai/data-categories/mobile-location-data* [*https://perma.cc/X8FH-GY9Y*].

[284] Sherman et al., *supra* note 6.

[285] *See, e.g.,* Thompson & Warzel, *supra* note 44.

[286] *See, e.g., The Guide to Getting & Using Your Health Records,* Off. Nat'l Coordinator for Health Info. Tech., *https://www.healthit.gov/how-to-get-your-health-record/* [*https://perma.cc/K2ZH-7VTW*]; *Dick Cheney Feared Assassination Via Medical Device Hacking: 'I Was Aware of the Danger,'* ABC News (Oct. 19, 2023), *https://abcnews.go.com/US/vice-president-dick-cheney-feared-pacemaker-hacking/story?id=20621434* [*https://perma.cc/Q779-MESR*].

[287] *See* Trisha Torrey, *How to Get Your Medical Records,* Verywell Health (May 11, 2023), *https://www.verywellhealth.com/how-to-get-copies-of-your-medical-records-2615505* [*https://perma.cc/2VY5-PXJA*].

[288] *See, e.g., Dick Cheney Feared Assassination Via Medical Device Hacking, supra* note 286.

[289] John J. Palmieri & Theodore A. Stern, *Lies in the Doctor-Patient Relationship,* 11 Prim. Care Companion J. Clinical Psychiatry 163, 165 (2009), *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2736034/* [*https://perma.cc/AH9L-FD5K*].

[290] *Health Information Privacy Law and Policy,* Off. Nat'l Coordinator for Health Info. Tech., *https://www.healthit.gov/topic/health-information-privacy-law-and-policy* [*https://perma.cc/2XHZ-UPFE*].

[291] Trisha Torrey, *Who Can Access Your Medical Records?* VeryWell Health (Mar. 11, 2022), *https://*

• *Availability:* High sensitivity. Personal health data is considered highly private and is well protected by privacy legislation. Data is shared as part of clinical trials, but access to such data is recognized as a continuing challenge within the healthcare community.[292] Furthermore, health data remains highly valuable to cyber criminals on the dark web, as compared to data such as credit card numbers and Social Security numbers, pointing to the general difficulty in obtaining this information in bulk quantities.[293]

• *Volume:* Varied sensitivity. As discussed, personal health data generally contains large amounts of data of varying formats and structures, ranging from the highly structured and technical information in lab results, to the more unstructured data, such as x-ray images and magnetic resonance imaging scans. Such variation means the amount of information may range from very small, such as the results of a single test, to very voluminous, such as a complete medical history. The volume of elements such as progress notes is also increasing, further expanding variability.[294]

• *Velocity:* Moderate-to-low sensitivity. As discussed, personal health data contains a variety of different types of information, but many of these records are lab tests, diagnostics, and other treatment information that may be less useful to analysts. However, certain pieces of information of enduring value—such as information on chronic disease and hereditary conditions—may be mixed in with other pieces of information, somewhat raising the overall sensitivity.

• *Quality:* Low sensitivity. Personal health records vary widely in terms of data type, quantity, precision, and consistency,[295] making personal health data less suitable for automated machine analysis than other types of data. Analysts or automated systems may not be able to draw useful conclusions without a great deal of context surrounding highly technical diagnostic data. ''Note bloat''—unnecessarily lengthy information—is a recognized issue within the medical community, indicating the ongoing challenge of obtaining quality, valuable information.[296] Much of the useful information may be contained in generalized diagnostics, particularized forms, and images that analysts may not be able to easily transform into useful conclusions, particularly if patients are not being truthful.[297]

5. Personal Financial Data

The Department of Justice assesses that personal financial data is the fifth most sensitive category of sensitive personal data. To conduct the analysis, the Department considered data linked directly with personal financial accounts (*e.g.,* records with account numbers and names), data included in financial applications such as data used to apply for mortgages or loans (*e.g.,* credit history), and related data routinely exchanged during a transaction (*e.g.,* account numbers, routing numbers). Personal financial data includes records that are confidential (*e.g.,* complete bank account information, including name). Personal financial data includes a variety of data types with varying sensitivity and moderate sensitivity overall based primarily on the purpose, changeability, availability, and quality characteristics below:

• *Purpose:* Moderate sensitivity. Financial institutions must uniquely identify and verify the identity of individuals both to track financial flows and to comply with regulations such as anti-money laundering.[298] In order to do this, they store a mix of data that is useful for identifying individuals. Other categories of financial data, such as credit or consumer reports, provide data that can be useful for characterizing behavior or grouping individuals into categories.[299] Today, most individuals leave a digital trail through their purchases and other financial activities, revealing behaviors, activities, and patterns of life.[300] They provide insight into their financial condition, personal preferences, habits, and concerns through brokerage activity, savings account information, and insurance records. Foreign intelligence services could derive other sensitive personal data, such as workplace and daily life habits, including vulnerabilities in an individual's personal life that may be leveraged to coerce that individual into recruitment by a foreign intelligence service, from financial transaction data.[301] Use of a financial instrument to purchase products or services reveals spending habits and patterns of life that help our adversaries target individuals and groups for intelligence recruitment, espionage, and influence. Debt, creditworthiness, and financial troubles provide points of leverage for coercion, blackmail, and influence.

• *Changeability:* Moderate-to-high sensitivity. Financial information on an individual is recorded and maintained by financial institutions, which depend on possessing reliable and accurate information. However, individuals do have some ability to change their financial identifiers by, for example, closing one account and opening another. Additionally, the continued existence of money laundering as a law enforcement issue demonstrates that financial information can be, to some extent, controlled or manipulated by an individual.[302]

• *Control:* Moderate sensitivity. Financial information and records are managed and maintained by centralized financial institutions. Credit cards and checks leave a history with the financial institution, but individuals have the power to pay in cash or other anonymized methods and not reveal transactions to these financial institutions.[303] Ultimately, this

www.verywellhealth.com/who-has-access-to-your-medical-records-2615502 [*https://perma.cc/BX52-5URC*].

[292] Sonali Kochhar et al., *Clinical Trial Data Sharing: Here's the Challenge,* 9 BMJ Open (2019), *https://bmjopen.bmj.com/content/9/8/e032334* [*https://perma.cc/392P-PVKN*].

[293] Sanjay Cherian, *Healthcare Data: The Perfect Storm,* Forbes (Jan. 14, 2022), *https://www.forbes.com/sites/forbestechcouncil/2022/01/14/healthcare-data-the-perfect-storm* [*https://perma.cc/DR6V-D7QY*].

[294] Adam Rule et al., *Length and Redundancy of Outpatient Progress Notes Across a Decade at an Academic Medical Center,* 4 JAMA Network Open (July 19, 2021), *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8290305/* [*https://perma.cc/7NA8-7Y9N*].

[295] *See, e.g.,* Alex Roehrs et al., *Personal Health Records: A Systematic Literature Review,* 19 J. Med. Internet Rsch. under sections titled Overview, Electronic Health Records, and Personal Health Records (Jan. 6, 2017), *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5251169/* [*https://perma.cc/T6MA-29VB*].

[296] *See Cures for Note Bloat,* ForeSee Medical (June 9, 2023), *https://www.foreseemed.com/blog/note-bloat-cures* [*https://perma.cc/AB34-CYGL*].

[297] Palmieri & Stern, *supra* note 289.

[298] *Frequently Asked Questions (FAQ) Regarding Anti-Money Laundering (AML),* FINRA, *https://www.finra.org/rules-guidance/key-topics/aml/faq* [*https://perma.cc/Z9TK-WBRW*].

[299] Barry Paperno, *How Credit Scores Predict Your Behavior,* Yahoo! Finance (May 24, 2013), *https://finance.yahoo.com/news/credit-scores-predict-behavior-113006994.html* [*https://perma.cc/GC4S-6H67*].

[300] Nicholas Anthony, Policy Analysis No. 945, *The Right to Financial Privacy,* CATO Inst. (May 2, 2023), *https://www.cato.org/policy-analysis/right-financial-privacy#conclusion* [*https://perma.cc/5K3E-BUPF*] (''Today, technology is an integral part of modern life: Americans use credit or debit cards for nearly all purchases, acquire loans directly on their phones, and leave a digital trail nearly everywhere they go.'').

[301] Carola Westermeier, *Money Is Data—The Platformization of Financial Transactions,* 23 Info., Commc'n & Soc'y 2047, 2050–52 (2020), *https://www.tandfonline.com/doi/full/10.1080/1369118X.2020.1770833* [*https://perma.cc/TD9J-UF9U*].

[302] *Examples of Money Laundering Techniques,* LexisNexis (May 4, 2023), *https://www.lexisnexis.com/blogs/gb/b/compliance-risk-due-diligence/posts/examples-money-laundering* [*https://perma.cc/6MHE-U83S*].

[303] *See, e.g.,* Edvardas Mikalauskas, *The Ultimate Guide to Safe and Anonymous Online Payment*

Continued

information reflects the activity of individuals, leaving it partly in their control.

• *Availability:* Moderate sensitivity. The sharing of certain types of information maintained by financial institutions is controlled by privacy regulations.[304] However, credit card, debit card, and bank account numbers, and other financial identifiers and information, are routinely exchanged as a matter of course in commercial transactions; credit reports are regularly used by financial institutions and businesses as part of background checks; and transaction data is provided to marketing and third-party data analytics organizations.[305] Credit cards and online financial account credentials can command between $15 and $200 on the dark web, as compared with Social Security numbers, which command less than $10.[306]

• *Volume:* Moderate-to-low sensitivity. Over 100 million credit card transactions occur in the United States each day.[307] While each transaction contains a small amount of information, this total transaction volume represents a massive dataset that analysts must mine to achieve useful results. Other types of information, such as data in credit reports, can contain information in a wide variety of formats that may be bulkier to manage and store.

• *Velocity:* Varied sensitivity. Analysts can use certain pieces of data, such as long-term loans, for a very long time. However, other pieces of information, such as information on individual transactions, may lose their value to an analyst over a short period of time.

• *Quality:* Moderate sensitivity. Analysts usually value personal financial data not for the information itself, but for what it can reveal about an individual's behavior.[308] As a result, some analysis is usually required to make it useful. Additionally, financial records such as credit reports can contain inaccurate information or make erroneous connections between individuals and assets.[309]

6. Covered Personal Identifiers

The Department of Justice assesses that covered personal identifiers are the sixth most sensitive category of sensitive personal data. Covered personal identifiers come from a variety of contexts and are of varying quality. For example, people have used certain types of covered personal identifiers (*e.g.,* Social Security numbers) for decades, and numerous entities collect them, making them more available than other categories of data. Other types of covered personal identifiers (*e.g.,* advertising IDs) are distributed widely and only useful when collected in very large volumes and linked to other pieces of data.[310] The variety and variability of this category makes it inherently more difficult to characterize across the board than other categories. Based primarily on the purpose, changeability, and velocity characteristics below, the Department assesses covered personal identifiers to have low sensitivity relative to the other categories of sensitive personal data:

• *Purpose:* Moderate sensitivity. As stated in the proposed rule, covered personal identifiers are pieces of data that can be useful for identifying individuals, making them inherently sensitive. However, covered personal identifiers include pieces of information that are uniquely identifying (*e.g.,* Social Security numbers) as well as those that are deliberately designed to be anonymous (*e.g.,* advertising identifiers).[311] Covered personal identifiers and unique IDs can be used to link other datasets containing more directly exploitable information.[312] For example, they can help link databases of habitual visitors to gambling sites with debt collection records or a database of government records. They could link advertising IDs, IP addresses, and SIM card numbers to personal mobile devices, home addresses, and government mobile devices. However, in general, covered personal identifiers are primarily useful as identifiers, reducing their overall sensitivity because they themselves reveal little information.

• *Changeability:* Moderate-to-low sensitivity. As a category, they cover a range of data points that differ in terms of ease of change. For example, Social Security numbers are difficult to change, requiring evidence that an individual is in danger from domestic violence, other abuse, or identity theft.[313] In contrast, account identifiers and passwords can be changed at a user's discretion. Many covered personal identifiers, including passport numbers, device IMEIs, and addresses, do change on a semi-regular basis as passports are reissued, devices are replaced, and individuals move.

• *Control:* Moderate-to-low sensitivity. Some covered personal identifiers—particularly government-issued identifiers such as Alien Registration Numbers and Social Security numbers or financial identifiers such as account information—are fully outside the control of an individual. Others are fully controlled by an individual, including email addresses and account identifiers. Still other covered personal identifiers such as phone numbers may be issued by a third party, but an individual can change them at will.

• *Availability:* Low sensitivity. Covered personal identifiers such as phone numbers and home addresses have been used as unique identifiers in a variety of systems, ranging from customer loyalty trackers to tax records. Many are available as part of the public record.[314] Technical covered personal

Methods in 2024, Cybernews (Dec. 12, 2023), *https://cybernews.com/resources/the-ultimate-guide-to-safe-and-anonymous-online-payment-methods/* [*https://perma.cc/5EX5-8YFC*].

[304] *See, e.g.,* Gramm-Leach-Bliley Act tit. V, 15 U.S.C. 6801–09; *Privacy Rule Handbook,* Fed. Deposit Ins. Corp. (Aug. 11, 2023), *https://www.fdic.gov/regulations/examinations/financialprivacy/handbook/index.html* [*https://perma.cc/NK9U-MVFY*].

[305] *See, e.g.,* R.J. Cross, *How Mastercard Sells Its 'Gold Mine' of Transaction Data,* U.S. PIRG (June 17, 2024), *https://pirg.org/edfund/resources/how-mastercard-sells-data/* [*https://perma.cc/N4T8-P3ZG*].

[306] Paul Bischoff, *Dark Web Prices for Stolen PayPal Accounts Up, Credit Cards Down: Report,* Comparitech (Aug. 12, 2023), *https://www.comparitech.com/blog/vpn-privacy/dark-web-prices/* [*https://perma.cc/88HM-2VZK*].

[307] Erica Sandberg, *The Average Number of Credit Card Transactions per Day & Year,* iMerchant Direct (Nov. 5, 2020), *https://www.imerchantdirect.com/news/number-of-credit-card-transactions-per-day-year* [*https://perma.cc/NVZ8-M3PR*].

[308] Alessio Balduini et al., *Combining Financial and Behavioral Information to Predict Defaults for Small and Medium-Sized Enterprises: A Dynamic Weighting Approach,* Moody's Analytics (Sept. 2017), *https://www.moodysanalytics.com/articles/2017/combining-financial-and-behavioral-information* [*https://perma.cc/X8DS-WPZB*]; Luke Goldsten, *Rollups: The Big Data Machine Driving Online Sports Betting,* Am. Prospect (Apr. 4, 2022), *https://prospect.org/power/rollups-big-data-machine-driving-online-sports-betting/* [*https://perma.cc/AZ97-H4TW*].

[309] *Is My Credit Report Accurate? For Over 40 Million Americans, the Answer Is No,* Am. Bankr. Inst., *https://www.abi.org/feed-item/is-my-credit-report-accurate-for-over-40-million-americans-the-answer-is-no* [*https://perma.cc/462F-UMEN*].

[310] Priv. Int'l, *Examples of Data Points Used in Profiling,* 3–12 (2018), *https://privacyinternational.org/sites/default/files/2018-04/data%20points%20used%20in%20tracking_0.pdf* [*https://perma.cc/LF63-XUDT*].

[311] *Are Advertising Unique IDs Anonymous?,* Panda Sec. (July 21, 2021), *https://www.pandasecurity.com/en/mediacenter/advertising-ids/* [*https://perma.cc/ANA8-JE2H*].

[312] Priv. Int'l, *supra* note 310.

[313] *Is It Possible to Get a New Social Security Number?,* AARP (Apr. 8, 2022), *https://www.aarp.org/retirement/social-security/questions-answers/new-number.html* [*https://perma.cc/X759-P6LF*].

[314] *See, e.g.,* Brian Fung, *DC Makes It Shockingly Easy to Snoop on Your Fellow Voters,* Wash. Post (June 14, 2016), *https://www.washingtonpost.com/news/the-switch/wp/2016/06/14/d-c-s-board-of-elections-makes-it-shockingly-easy-to-snoop-on-your-fellow-voters/* [*https://perma.cc/5A2J-VNAZ*]; How Your Phone Number is Exposed: Phone

identifiers such as IP addresses are necessarily widely available as a matter of technical necessity.

- *Volume:* Low sensitivity. Online data-brokerage firms advertise datasets of mobile advertising IDs containing hundreds of millions to billions of records.[315] Tens of millions of Social Security numbers are routinely found on the dark web, suggesting the large volumes in which these data points are stored and shared by companies.[316] Companies such as Twitter (now X) hold the phone numbers and email addresses of more than 100 million individuals.[317] As these examples demonstrate, covered personal identifiers are routinely held and used in massive volumes. At such large volumes, this type of data tends to be less sensitive because it reduces the ability of an adversary to identify a specific individual (such as distinguishing between people who have the same name, have lived at the same address, etc.), absent other data that can be used to narrow down and link the identifiers to individuals.
- *Velocity:* Moderate-to-low sensitivity. Covered personal identifiers such as Social Security numbers and names can be quite persistent, changing infrequently or not at all over an individual's lifetime. Covered personal identifiers like mobile advertising IDs cease to be useful in as little as 7 to 8 months.[318] In general, the useful lifespan of many covered personal identifiers is limited. Only a few covered personal identifiers follow an individual over a lifetime, while many have lifespans measured in weeks to months, reducing the overall sensitivity of the category.
- *Quality:* Low sensitivity. For example, an individual user may have multiple mobile advertising IDs across multiple devices. Advertising specialists assert that 91 percent of companies have data quality issues, including from outdated data and user-error mistakes.[319] Individuals may also make and use throwaway email accounts to avoid spam.[320] Major technology companies, such as Apple, offer the ability to create relay emails specifically to obfuscate certain underlying covered personal identifiers.[321]

B. Grouping the Categories Into Tiers by Similar Sensitivity

Based on this ranking, the Department grouped the categories of sensitive personal data into four tiers based on how similar or dissimilar, in terms of sensitivity, each category is compared to the other. Human genomic data, the most sensitive category, is unique and substantially more sensitive than biometric data due to its lower changeability and velocity. As a result, the Department placed human genomic data on its own in the first tier. While not as sensitive as human genomic data, biometric identifiers and precise geolocation data are generally more sensitive than either personal health or personal financial data because the data is more structured, making it more useful for machine-based analysis. Biometric identifiers and precise geolocation data also identify individuals with more precision than personal health data or personal financial data, making the results of machine-based analysis more valuable to human analysts. As a result, the Department grouped biometric identifiers and precise geolocation data together into the second tier and grouped personal financial data and personal health data together into the third tier. Finally, compared to personal financial data or personal health data, covered personal identifiers are more varied in terms of use, making them less useful to foreign intelligence services. As a result, the Department grouped covered personal identifiers into the fourth tier.

To help verify the relative sensitivities and tiered groupings yielded by the seven-factor analysis, the Department compared the results of this analysis to other circumstances in which the Federal Government or state governments have treated these categories of data as sensitive. To start, the Department examined over 50 transactions reviewed by CFIUS in which the government identified, and took action to address, a risk to national security posed by access to data by countries of concern or persons subject to their ownership, direction, jurisdiction, or control. The Department examined the types and volumes of data involved in each CFIUS transaction to identify the lowest volumes of data that the government identified as a risk to national security posed by each of these transactions, which served as proxy for how sensitive CFIUS has generally considered each category of data with respect to identified national security risks relating to that data.

In the case of personal financial data, personal health data, and covered personal identifiers, the Department was able to identify enough CFIUS transactions to present a reasonable sample. It identified the following approximate numbers as the lowest volumes identified by CFIUS as presenting a national security risk warranting action in the context of the specific transactions involving sensitive personal data that CFIUS reviewed:

- Personal financial data: 16,000 individuals
- Personal health data: 85,000 individuals
- Covered personal identifiers: 100,000 individuals

Based on these data points, the Department confirmed that its sensitivity analysis of these three categories was consistent with previous CFIUS national security assessments, at least in the specific contexts of those case-by-case CFIUS reviews.

Because there was not a sufficiently large sample of CFIUS matters for human genomic data, biometric data, or precise geolocation data, and because there does not appear to be another national security program with relevant quantitative or qualitative data on this topic, the Department examined how the Federal Government and States treat these three remaining categories under privacy laws to help verify the results of its seven-factor assessment. While privacy laws and national security laws generally address different challenges associated with sensitive personal data, as explained in part IV of this preamble, there is some overlap in the ultimate harms that both seek to address. These privacy-based analogues thus help provide some indication of the relative capability of each category of sensitive personal data to be exploited and used to cause harm.

Number Leaks, Nat'l. Cybersec. All. (Aug. 25, 2023), *https://staysafeonline.org/online-safety-privacy-basics/how-your-phone-number-is-exposed/* (*https://perma.cc/4CL3-9WRW*).

[315] *See, e.g., MAID—PII Data: Best MAID—PII Datasets & Databases,* Datarade, *https://datarade.ai/search/products/maid-pii-data* [*https://perma.cc/6NWA-YEBK*].

[316] *See* Chloe Veltman, *Millions of Customers' Data Found on Dark Web in Latest AT&T Data Breach,* NPR (Mar. 30, 2024), *https://www.npr.org/2024/03/30/1241863710/att-data-breach-dark-web* [*https://perma.cc/GAD6-R9KU*].

[317] *See* Complaint ¶ 29, *United States* v. *Twitter, Inc.,* No. 22–cv–03070 (N.D. Cal. May 25, 2022), ECF No. 1, *https://www.ftc.gov/system/files/ftc_gov/pdf/2023062TwitterFiledComplaint.pdf* [*https://perma.cc/4Z9J-5N3H*].

[318] *3 Uses for Mobile Advertising IDs to Copy Today,* FullContact (Feb. 21, 2022), *https://www.fullcontact.com/blog/2022/02/21/mobile-advertising-id/* [*https://perma.cc/RR89-25HL*].

[319] Barley Laing, *Why Customer Loyalty Starts with Clean Data,* Advert. Week, *https://advertisingweek.com/why-customer-loyalty-starts-with-clean-data/* [*https://perma.cc/LJ3G-9M7F*].

[320] Vivian McCall, *How to Make a Throwaway Email Account to Avoid Spam from the websites You Sign up for,* Bus. Insider (Dec. 22, 2020), *https://www.businessinsider.com/guides/tech/how-to-make-a-throwaway-email-account* [*https://perma.cc/27C4-DQJQ*].

[321] *Communicating Using the Private Email Relay Service,* Apple Dev., *https://developer.apple.com/documentation/sign_in_with_apple/sign_in_with_apple_js/communicating_using_the_private_email_relay_service* [*https://perma.cc/62AC-K9HK*].

In the case of human genomic data, the Department confirmed its assessment that this category of data is more sensitive than the three previously mentioned categories of data (covered personal identifiers, personal financial data, and personal health data) by evaluating comparative data from the FTC. The FTC has taken action against companies making deceptive privacy claims on cases involving the human genetic data of as few as 2,600 individuals.[322] In doing so, the FTC's complaint alleged that the company's ''disregard for the basic security'' of this data caused it to be ''publicly exposed online,'' [323] revealing, among other things, ''the level of risk for having or developing certain health conditions.'' [324] The FTC also explained that this kind of ''DNA data is sensitive because it's about who'' a person is and is ''so sensitive there's a law to protect you from discrimination based on genetic information when you're trying to get work or health insurance.'' [325] In contrast, eight other FTC cases between 2021 and 2023 involving only covered personal identifiers, personal financial data, or personal health data involved data on one million or more individuals. The fact that the FTC took action in a case involving a significantly lower amount of compromised human genomic data supports the Department's assessment that human genomic data is substantially more sensitive than other data types.

In the case of biometric data, the Department confirmed its assessment with reference to State legislation. Three States—Washington,[326] Texas,[327] and Illinois [328]—have prohibited the sale, lease, or disclosure of biometric identifiers for purposes other than the provision of a specific commercial service, such as confirming a consumer-requested financial transaction. Massachusetts is also contemplating such a law at the time of this proposed rule.[329] The legislative action in these cases supports the Department's assessment that the transfer of even very small amounts of biometric data could prove highly damaging and thus that this data should be subject to a lower threshold.

In the case of geolocation data, the Department confirmed its assessment with reference to other government actions and reporting suggesting that even small amounts of geolocation data could be sensitive. The FTC charged two companies with causing injury to consumers by selling geolocation data that did not exclude information on sensitive locations, such as reproductive health clinics, places of worship, and addiction recovery facilities, and issued an order banning one of those companies from selling data without consumer consent.[330] It also noted a data breach that involved 2,200 customers as part of its action against a company that harvested and shared data on people's physical movements.[331] The FCC has also levied fines for selling location data without customer consent.[332] The National Security Agency has noted the importance of limiting location data exposure.[333] Congressional testimony has highlighted how commercial datasets can be used to precisely identify individuals in sensitive national security roles.[334] The Massachusetts State legislature is considering a bill at the time of this proposed rule that would ban the sale of phone location data.[335] These comparisons all support the Department's assessment that this type of data is relatively more sensitive than other types of data, such as personal identifiers.

C. Proposed Bulk Thresholds for Each Tier

The Department of Justice developed numerical thresholds using the four tiers of sensitivity based on the number of individuals included in a dataset. In the ANPRM, the Department set the overall upper limit for these thresholds at one million individuals.[336] As explained in the ANPRM, within each group, the Department set a potential upper and lower limit for each of the bulk thresholds, relying on orders-of-magnitude differences to develop preliminary judgments.

The Department sought input on the thresholds from the public in response to the ANPRM. Commenters expressed a wide variety of general concerns regarding the ranges of the potential bulk thresholds. Some commenters stated that the potential thresholds were too high, some that they were too low, some that the thresholds should be zero, and some that relying on thresholds was objectionable for other reasons. None of the comments, however, provided any actionable data points, use cases, or evidence that would support an alternative analytical framework or support adopting one particular threshold over another. Given that lack of specificity, the Department (along with the Department of Commerce) followed up individually with each commenter on this topic to seek any additional information available that informed their comments, as described in part III of this preamble. Those engagements did not yield any substantially new qualitative or quantitative information to reliably inform the selection of the proposed bulk thresholds.

Based on this analysis and public comment, the proposed rule would set the following bulk thresholds:

- *Human genomic data:* More than 100 U.S. persons.

---

[322] Complaint ¶ 28, *1Health.io, Inc.,* No. C–4798 (F.T.C. Sept. 6, 2023), *https://www.ftc.gov/system/files/ftc_gov/pdf/1Health-Complaint.pdf* [*https://perma.cc/W5SZ-CE3A*].

[323] *Id.*

[324] *Id.* ¶ 9.

[325] Jim Kreidler, *Keep People's Sensitive DNA Information Private,* Fed. Trade Comm'n (June 16, 2023), *https://consumer.ftc.gov/consumer-alerts/2023/06/keep-peoples-sensitive-dna-information-private* [*https://perma.cc/VLC4-JYKM*].

[326] Biometric Identifiers, Wash. Rev. Code 19.375, *https://app.leg.wa.gov/RCW/default.aspx?cite=19.375&full=true* [*https://perma.cc/2GZM-6FEG*].

[327] Biometric Identifiers, Tex. Bus. & Com. Code 503.001, *https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm* [*https://perma.cc/F2WW-ZNR7*].

[328] Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14 (2008), *https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57* [*https://perma.cc/KMD8-QP8D*].

[329] Act to Protect Biometric Information, H. 63, 193d. Gen. Ct. (Mass. 2003), *https://malegislature.gov/Bills/193/H63* [*https://perma.cc/26GH-JTCZ*].

[330] Press Release, Fed. Trade Comm'n, *FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations* (Aug. 29, 2022), *https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other* [*https://perma.cc/G6L6-G6XL*].

[331] Press Release, Fed. Trade Comm'n, *FTC Bans SpyFone and CEO from Surveillance Business and Orders Company to Delete All Secretly Stolen Data* (Sept. 1, 2021), *https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-bans-spyfone-ceo-surveillance-business-orders-company-delete-all-secretly-stolen-data* [*https://perma.cc/SG4B-P6SV*].

[332] Derek B. Johnson, *FCC Takes $200 Million Bite Out of Wireless Carriers for Sharing Location Data,* CyberScoop (Apr. 29, 2024), *https://cyberscoop.com/fcc-fines-wireless-carriers-200-million/* [*https://perma.cc/9UKR-4KXY*].

[333] Nat'l Sec. Agency, PP–20–0535, *Limiting Location Data Exposure* (Aug. 2020), *https://media.defense.gov/2020/Aug/04/2002469874/-1/-1/0/CSI_limiting_location_data_exposure_final.pdf* [*https://perma.cc/763S-8D5T*].

[334] *Data Brokerage, the Sale of Individuals' Data, and Risks to Americans' Privacy, Personal Safety, and National Security: Hearing Before the Subcomm. on Oversight & Investigations of the H. Comm. on Energy & Com.,* 118th Cong. (2023) (statement of Justin Sherman, Senior Fellow and Research Lead, Data Brokerage Project, Sanford School of Public Policy), *https://d1dth6e84htgma.cloudfront.net/Sherman_Testimony_4_19_23_b40d947a8e.pdf* [*https://perma.cc/9ACJ-ZT8R*].

[335] Shanklin, *supra* note 279.

[336] 89 FR 15786; *cf.* 31 CFR 800.241(a) (defining sensitive personal data to include ''identifiable data'' that a U.S. business collects or maintains ''on greater than one million individuals'' during a relevant 12-month period).

• *Biometric identifiers and precise geolocation data:* More than 1,000 U.S. persons.

• *Personal health data and personal financial data:* More than 10,000 U.S. persons.

• *Covered personal identifiers:* More than 100,000 U.S. persons.

The proposed bulk thresholds for all the categories of sensitive personal data except human genomic data are approximately the middle order of magnitude of the preliminary ranges identified in the ANPRM (*e.g.,* the proposed threshold of 1,000 U.S. persons for biometric identifiers is the middle order of magnitude in the ANPRM's range of 100 to 10,000).[337] Given the high sensitivity of human genomic data and the significant additional national security risks posed by human genomic data beyond counterintelligence risks, the proposed bulk threshold for human genomic data is the lowest order of magnitude in the preliminary range identified in the ANPRM. These proposed bulk thresholds are generally consistent with the order of magnitude of the minimum number of individuals in a dataset that the United States Government and other actors have treated as presenting a national security risk or as otherwise sensitive in the use cases and comparisons described in part V.B of this preamble.

The Department has considered whether the potential economic impact should affect our choice of thresholds for the purpose of defining ''bulk'' in these regulations and has determined it should not. First, the Department expects that the proposed rule will likely have some economic impact with respect to the prohibitions and restrictions on covered data transactions that have been determined to pose an unacceptable national security risk. The Department seeks to avoid and minimize unintended economic impacts on activities that do not present such national security risk. Neither the Department nor commenters have identified any actionable data or analysis suggesting that the choice of thresholds above zero is reasonably likely to result in unintended downstream impacts, as explained further in part VII.A of this preamble.

Second, based on the information provided to the Department and the Department's own analysis to date, it seems unlikely that the data or analysis would be detailed and representative enough to reasonably affect the choice of any specific thresholds within the ranges identified in the ANPRM. While it is theoretically possible that choosing a higher (or lower) threshold would correspondingly affect both the numbers of captured transactions and the resultant costs, it is also possible that a meaningfully significant sample size of U.S. persons conducting prohibited and restricted transactions at volumes that generally exceed the upper end of the ranges in the ANPRM. There is no known, reliable qualitative or quantitative data that objectively favors adopting one of those likely possibilities at this time. For example, the average volume and distribution of volumes of human genomic data in covered data transactions between U.S. persons and countries of concern (or covered persons) is unknown. Because there is no data available to determine how often, for example, U.S. persons engage in such transactions at volumes above 1,000 U.S. persons as compared to 100, there is insufficient data to support a conclusion that the choice between 100 and 1,000 will meaningfully impact the number of transactions subject to the proposed rule. Accordingly, the Department declines to deviate from the risk-based analysis at this time.

VI. Interpretation of ''Information or Informational Materials'' in IEEPA

The Department proposes exercising its delegated statutory authority to define ''information or informational materials'' in 50 U.S.C. 1702(b)(3). Under IEEPA, ''[t]he President may issue such regulations, including regulations prescribing definitions, as may be necessary for the exercise of the authorities granted by this chapter.'' [338] As courts have held, this provision explicitly ''authorize[s] the Executive Branch to define the statutory terms of IEEPA,'' and definitions promulgated by an agency that has been delegated this authority thus ''carry the force of law'' subject to judicial deference.[339] Section 2(b) of the Order delegated this statutory authority to the Attorney General, and the Department proposes to exercise this authority to define ''information or informational materials'' as follows.

To implement 50 U.S.C. 1702(b)(3), the Department proposes defining ''information or informational materials'' as limited to expressive material and including publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds.[340]

The proposed rule would adopt two exclusions to this definition from existing OFAC regulations and clarify the definition's application to non-expressive materials. First, as previewed in the ANPRM and explained in detail below, the Department's proposed rule would clarify that the phrase ''information or informational materials'' is limited to expressive material, consistent with the purpose of 50 U.S.C. 1702(b)(3) to protect materials involving the free exchange of ideas from regulation under IEEPA. *See* § 202.226. The definition of ''information or informational materials'' does not include non-expressive data—*i.e.,* data that is not intended to communicate any idea. The statute therefore permits the President, and the Attorney General as his delegee under the Order, to regulate transactions involving the export of sensitive personal data or government-related data because this data is not expressive and therefore falls outside the scope of 50 U.S.C. 1702(b)(3) (''the Berman Amendment''). Second, the proposed definition would, consistent with OFAC regulations,[341] exclude information or informational materials that are 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. Third, the proposed definition incorporates the statutory exemption for items controlled for export to the extent that such controls promote the nonproliferation or antiterrorism policies of the United States, or with respect to which acts are prohibited by 18 U.S.C. chapter 37. The definition's application to non-expressive material and exclusion for materials not fully created and in existence are discussed in further detail below.

A. The Berman Amendment Is Intended To Protect the Free Exchange of Ideas

As noted above, § 202.226(a) of the proposed rule clarifies that ''information or informational materials'' is limited to expressive material rather than

[337] 89 FR 15786.

[338] 50 U.S.C. 1704.

[339] *Zarmach Oil Servs., Inc.* v. *U.S. Dep't of Treas.,* 750 F. Supp. 2d 150, 156 (D.D.C. 2010); *see also, e.g., Holy Land Found.* v. *Ashcroft,* 333 F.3d 156, 162–63 (D.C. Cir. 2003); *United States* v. *Lindh,* 212 F. Supp. 2d 541, 562–63 & n.52 (E.D. Va. 2002); *Consarc Corp.* v. *U.S. Dep't of Treas., Off. of Foreign Assets Control,* 71 F.3d 909, 914–15 (D.C. Cir. 1995); *Consarc Corp.* v. *Iraqi Ministry,* 27 F.3d 695, 701 (D.C. Cir. 1994).

[340] *See, e.g.,* 31 CFR 544.304(a); 31 CFR 547.314(a)(1); 31 CFR 560.315(a); 31 CFR 576.306(a); 31 CFR 594.305(a).

[341] *See, e.g.,* 31 CFR 560.210(c)(2), 560.210; *United States* v. *Amirnazmi,* 645 F.3d 564, 587 (3d Cir. 2011).

including every piece of data that might be characterized technically or colloquially as ''information or informational materials.'' This interpretation is consistent with the statute's text and purpose, as demonstrated by legislative history and context, as well as judicial interpretations.

The text indicates that the Berman Amendment's scope is properly limited to expressive materials. The provision restricts authority under IEEPA to regulate imports and exports ''regardless of format or medium of transmission, of any information or informational materials, including but not limited to, publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds.'' The specific examples accompanying the phrase ''information and informational materials''—publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds—reflect Congress' intent to protect the import or export of expressive speech and communicative works and mediums that may be carrying such expressive content. Although the statute provides that it is ''not limited to'' the articulated categories of information or specified mediums, the general term ''information or informational materials'' must be read in the context of those examples and should not be read to extend to dissimilar categories of information to those specifically articulated.[342] Because those examples overwhelmingly relate to expressive materials, the term ''information or informational materials'' is similarly limited under the established interpretive doctrine of *noscitur a sociis.*

Congress enacted the Berman Amendment in 1988 and expanded it in 1994,[343] and the initial version of the Berman Amendment passed in 1988 further supports this argument. It amended IEEPA to state that the President's authority under the statute did not include the authority ''to regulate or prohibit, directly or indirectly . . . the importation from any country, or the exportation to any country, whether commercial or otherwise, of publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, or other informational materials. The specified items shared the common attribute of having the primary or exclusive purpose of conveying expressive information, and the catch-all term ''other informational materials'' therefore carried that same limitation under the canon of *ejusdem generis.*[344] This interpretation is further reinforced by the statute's use of ''other'' before ''informational materials,'' indicating a commonality with the enumerated items. As further discussed below, there is no indication that, in amending the 1988 text, Congress sought to deviate from that understanding. The 1994 amendment that enacted the current version of the Berman Amendment was titled ''Free Trade in Ideas,'' indicating the provision's reach and orientation toward expressive and communicative materials.[345] The statute includes an accompanying provision providing ''the sense of the Congress that the President should not restrict travel or exchanges for informational, education, religious, cultural, or humanitarian purposes or for public performances or exhibitions.'' [346] Together, these features confirm that the ''information or informational materials'' covered by the Berman Amendment are limited to the kind of expressive information that is central to the free exchange of ideas; the Berman Amendment is not intended to broadly encompass every piece of data that might technically or colloquially be described as ''information.''

The proposed interpretation is consistent with Congress' purpose in enacting the Berman Amendment. As one court explained shortly after the Berman Amendment's initial enactment in 1988, there is an ''obvious First Amendment orientation of the words 'informational materials.' '' [347] Other courts have reached similar conclusions about the Berman Amendment's purpose.[348] And courts have consistently upheld the Executive Branch's interpretations that distinguish between the types of informational materials that are covered or not covered, explaining that these reflect ''permissible interpretation[s]'' of the Berman Amendment ''in light of IEEPA's competing imperatives (*i.e.,* restricting material support for hostile regimes while encouraging the robust interchange of information).'' [349]

These courts' interpretations are grounded in the relevant historical and legislative context, which reflects Congress' intent to protect the free exchange of ideas. Before the Berman Amendment's enactment in 1988, the President's broad authority to regulate commerce with foreign countries under IEEPA and its predecessor and wartime sibling, the Trading with the Enemy Act of 1917 (''TWEA''), did not contain any statutory exception for ''information or informational materials,'' and the implementing regulations and licenses generally did not exempt information or informational materials from trade embargoes. Before and during the Cold War, the Executive Branch exercised these authorities to prohibit the importation of and dealing in certain merchandise. These general regulations applied to books, newspapers, and magazines originating in countries designated as enemy nations, such as Cuba, Vietnam, China, North Korea, and

[342] *See, e.g., Dubin* v. *United States,* 599 U.S. 110, 124–25 (2023) (' 'Under the familiar interpretive canon noscitur a sociis, a word is known by the company it keeps.' '[T]his canon is often wisely applied where a word is capable of many meanings in order to avoid the giving of unintended breadth to the Acts of Congress.' '' *McDonnell* v. *United States,* 579 U.S. 550, 568–69 (2016) (citations omitted).)

[343] Omnibus Trade and Competitiveness Act of 1988, Public Law 100–418, 2502(b), 102 Stat. 1107, 1371–72; Foreign Relations Authorization Act, Fiscal Years 1994 and 1995, Public Law 103–236, sec. 525, 108 Stat. 382, 474 (1994).

[344] *See, e.g., Bissonnette* v. *LePage Bakeries Park St., LLC,* 144 S. Ct. 905, 911 (2024) (explaining the ''familiar canon of statutory interpretation'' of *ejusdem generis* under which ''courts interpret a general or collective term at the end of a list of specific items in light of any 'common attributes shared by the specific items'') (cleaned up); *see also Ali* v. *Fed. Bureau of Prisons,* 552 U.S. 214, 225 (2008) (explaining that ''the inference embodied in ejusdem generis'' is ''that Congress remained focused on the common attribute when it used the catchall phrase'').

[345] Foreign Relations Authorization Act, Fiscal Years 1994 and 1995, Public Law 103–236, sec. 525, 108 Stat. 382, 474 (1994); *see, e.g., Merit Mgmt. Grp., LP* v. *FTI Consulting, Inc.,* 138 S. Ct. 883, 893 (2018) (section headings ''supply clues as to what Congress intended'').

[346] Public Law 103–236, sec. 525(a), 108 Stat. at 474.

[347] *Cernuda* v. *Heavey,* 720 F. Supp. 1544, 1550 (S.D. Fla. 1989).

[348] *See, e.g., United States* v. *Amirnazmi,* 645 F.3d 564, 586–87 (3d Cir. 2011); *Kalantari* v. *NITV, Inc.,* 352 F.3d 1202, 1205 (9th Cir. 2003) (explaining that the ''Berman Amendment was designed to prevent the executive branch from restricting the international flow of materials protected by the First Amendment''); *Marland* v. *Trump,* 498 F. Supp. 3d 624, 630 (E.D. Pa. 2020) (explaining that the Berman Amendment prevents the use of IEEPA to '' 'prohibit or restrict directly or indirectly the import or export of information that is protected under the First Amendment to the U.S. Constitution' '' (quoting H.R. Conf. Rep. No. 103–482, at 236)); *United States* v. *Griffith,* 515 F. Supp. 3d 106, 116–17 (S.D.N.Y. 2021); *United States* v. *Alavi,* CR 07–429–PHX–NVW, 2008 WL 1989773, at *1 (D. Ariz. May 5, 2008) (similar).

Two recent cases examining the provision are not to the contrary, since both cases dealt with only expressive materials. *See TikTok Inc.* v. *Trump,* 507 F. Supp. 3d 92, 98–100, 105 (D.D.C. 2020); *Marland* v. *Trump,* 498 F. Supp. 3d at 636. The United States Government did not dispute that these expressive communications exchanged on TikTok were ''informational materials'' under the Berman Amendment. *See TikTok,* 507 F. Supp. 3d, at 108.

[349] *See Amirnazmi,* 645 F.3d at 583, 587; *see also Griffith,* 515 F. Supp. 3d at 116–17; *Alavi,* 2008 WL 1989773, at *1.

Cambodia.[350] Absent a license granted by the Department of the Treasury, Americans could not import these materials into the United States or otherwise deal in them. To obtain such a license, an applicant had to show either that the books, magazines, and other materials were small-value ''bona fide gift[s]'' that did not provide ''any direct or indirect financial or commercial benefit'' to the enemy country or its nationals,[351] or that payment for the commercial import of the materials was made into a blocked account.[352] These prohibitions resulted in, for example, customs officials in the 1960s seizing ''packages containing English language books and newspapers produced in North Vietnam and China'' and refusing their entry until licenses were granted.[353]

Prior to the Berman Amendment's enactment, the United States Government took varying approaches to imports of expressive materials. The Executive Branch initially required licenses for U.S. imports of thousands of Cuban publications destined for Americans' personal use, and then later ''nominally allowed the importation of informational materials from Cuba but in reality, banned such importation by requiring that the importers make payment into blocked U.S. accounts.'' [354] Plaintiffs challenged these prohibitions and seizures under the First Amendment, but courts upheld them as constitutional on the grounds that the specific restrictions were merely ''incidental'' to the purpose of the regulations in restricting the flow of capital to enemy nations.[355] In contrast, the 1985 Nicaraguan embargo and 1986 Libyan embargo explicitly authorized the import of ''books, newspapers, magazines, films, phonograph records, tape recordings, photographs, microfilm, microfiche, posters, and similar materials'' and thus preserved Americans' ability to receive news, ideas, and other expressive content from those nations.[356]

Congress enacted the Berman Amendment against this regulatory and judicial backdrop and as an explicit ''reaction'' to the continued, and continually upheld, import restrictions on and seizures of ''shipments of magazines and books'' from most embargoed countries.[357] The Berman Amendment thus ''codif[ied] current practice . . . in the recent embargoes of trade with Nicaragua and Libya of exempting information materials and publications from import restrictions,'' [358] and used the same terms to do so (''publications,'' ''films,'' ''posters,'' and so on).

The legislative history confirms what context makes clear: The Berman Amendment was designed to reach expressive information protected by the First Amendment. The relevant House committee report explains that Congress intended the Berman Amendment to protect the import and export of expressive materials; the report favorably cited and quoted from an American Bar Association House of Delegates statement that ''no prohibitions should exist on imports to the United States of ideas and information if their circulation is protected by the First Amendment.'' [359] ''Accordingly,'' the report continued, ''these sections also exempt informational materials and publications from the export restrictions that may be imposed under these acts.'' [360] Senator Charles Mathias, the sponsor of an earlier bill that contained identical language removing restrictions on the import and export of information and that was the predecessor to the 1988 bill that enacted the Berman Amendment, explained that ''[t]he thread that ties all of these changes together'' is ''an ideal embodied in the first amendment [sic]: The removal of barriers that inhibit the free exchange of ideas across international frontiers.'' [361] Mathias emphasized not the specific doctrine of the First Amendment but rather its ''philosophy'' and ''ideal[s],'' including an ''open and robust debate in the marketplace of ideas.'' [362] As he further explained, ''this liberty, secured by the first amendment [sic], is thwarted by a number of laws which permit the Government to restrict the flow of information and the travel of individuals into and out of the United States,'' including ''restrict[ing] the import and export of information on the basis of the political doctrines contained in the information''—restrictions that the Berman Amendment was designed to address.[363]

In 1994, Congress updated the Berman Amendment in ways that reinforced the expressive focus of the term ''information or informational materials.'' Between the enactment of the Berman Amendment in 1988 and Congress' update in 1994, the Executive Branch had taken ''a narrow view of what constituted 'informational materials.' '' [364] Some of these restrictive Executive Branch interpretations were successfully challenged in court, and others were not. For example, the Department of the Treasury had interpreted the term ''informational materials'' as excluding ''intangible items, such as telecommunications transmissions'' (an interpretation that the courts approved),[365] and original art in the form of paintings (an

[350] *E.g.,* 31 CFR 515.204 (1985) (Cuba); 31 CFR 500.204 (1976) (China, North Korea, Vietnam, Cambodia).

[351] 31 CFR 515.544(b) (1985); 31 CFR 500.544 (1971).

[352] 31 CFR 515.545(b) (1985); 31 CFR 500.545 (1974).

[353] Burt Neuborne & Steven R. Shapiro, *The Nylon Curtain: America's National Border and the Free Flow of Ideas,* 26 Wm. & Mary L. Rev. 719, 730 (1985).

[354] *Walsh* v. *Brady,* 927 F.2d 1229, 1230 (D.C. Cir. 1991) (citing 31 CFR 515.545 (1987)); *see id.* at 731.

[355] *E.g., Veterans & Reservists for Peace in Vietnam* v. *Regional Comm'r of Customs,* 459 F.2d 676, 681 (3d Cir. 1972); *Teague* v. *Regional Comm'r of Customs,* 404 F.2d 441, 445–46 (2d Cir. 1968); *American Documentary Films, Inc.* v. *Sec'y of Treas.,* 344 F. Supp. 703, 706–07 (S.D.N.Y. 1972).

[356] *See* 31 CFR 540.536 (1985); 31 CFR 550.507 (1986); 31 CFR 550.411 (1986).

[357] *E.g., United States* v. *Amirnazmi,* 645 F.3d 564, 584 (3d Cir. 2011); *Kalantari* v. *NITV, Inc.,* 352 F.3d 1202, 1205 (9th Cir. 2003).

[358] *Walsh,* 927 F.2d at 1233 (quoting H.R. Rep. No. 40, 100th Cong., 1st Sess., pt. 3, at 113 (1987)); *see also id.* at 1233 n.3 (explaining that House report's incorporation into the Berman Act's official legislative history). The House committee report favorably cited the Nicaragua and Libya blockades, which had exempted certain ''informational materials such as books, records, and films.'' H.R. Rep. No. 100–40, pt. 3, at 71. The committee indicated an intention to ''codify'' that practice of ''exempting information materials and publications from import restrictions.'' *Id.* at 113.

[359] H.R. Rep. No. 100–40, *supra* note 358, at 113. Although this committee report accompanied H.R. 3, a predecessor bill that was vetoed in May 1988, *see* H.R. Doc. No. 100–200, 100th Cong., 2d Sess. (1988) (veto message), the President and Congress later agreed on a successor bill, H.R. 4848, that contained the same informational-materials exception as its predecessor and that ultimately was enacted into law as the Omnibus Trade and Competitiveness Act of 1988. Since this Act was ''derived largely from [the] predecessor bill'' and ''was not itself the subject of legislative debate,'' the Act ''specifically provide[d] that the legislative history for the predecessor bill, H.R. 3, generally is treated as its own legislative history.'' *Cernuda,* 720 F. Supp. at 1547–48; *see* Pub. L. 100–418, sec. 2(a), 102 Stat. 1107, 1119 (1988).

[360] H.R. Rep. No. 100–40, *supra* note 358, at 113.

[361] 132 Cong. Rec. 6550 (Mar. 27, 1986) (statement of Sen. Charles Mathias).

[362] *Id.* at 6550–51.

[363] *Id.; see Cernuda,* 720 F. Supp. at 1550 (explaining that ''[t]he point'' of the Berman Amendment was to ''totally exempt[ ] from prohibition or regulation the import of ideas and information protected by the First Amendment'' and thus ''eliminate[ ] the sort of constitutional questions that arose in cases like *American Documentary Films* and *Teague*'').

[364] *United States* v. *Amirnazmi,* 645 F.3d 583, 584 (3d Cir. 2011).

[365] Foreign Assets Control Regulations and Cuban Assets Control Regulations, 54 FR 5229 (Feb. 2, 1989) (codified at 31 CFR 500.206(a), (c), 500.332(b)(2) (1989)); 31 CFR 515.545(b) (2010) (prohibiting the remittance of royalties or other payments relating to works not yet in being); *see Capital Cities/ABC, Inc.* v. *Brady,* 740 F. Supp. 1007, 1011–12 (S.D.N.Y. 1990).

interpretation that the courts rejected).[366]

Congress responded to these regulatory and judicial decisions by ''clarify[ing]'' the text of the Berman Amendment through the passage of the Free Trade in Ideas Act.[367] As with the original 1988 version, the 1994 version of the Berman Amendment, as reflected in its text and legislative history, focuses on excluding expressive materials from regulation. In its 1994 changes, Congress added new examples of expressive materials to the Berman Amendment but did not otherwise expand its scope to include, for example, even non-expressive materials. First, Congress changed the term ''other informational materials'' to ''any information or informational materials.'' Second, Congress moved the new term from the end of the list to the beginning and expanded the list of materials, so that it now reads ''any information or informational materials, including but not limited to, publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds.'' [368] Third, Congress made explicit that the Berman Amendment applied to information or informational materials ''regardless of format or medium of transmission.'' [369]

The legislative history of these changes confirms that Congress intended to maintain the Berman Amendment's exclusive focus on protecting expressive materials from regulation under IEEPA and did not intend to exclude from the President's regulatory power the full scope of what colloquially might be understood to be information or informational materials. Among other things, the effect of these changes was, as the 1994 House report explained, to ''clarify'' the Berman Amendment by ''eliminating some of the unintended restrictive administrative interpretations of it.'' [370] For example, by adding the words ''regardless of format or medium of transmission,'' the 1994 amendment overrode the interpretation excluding intangible materials that was unsuccessfully challenged in *Capital Cities/ABC, Inc.* v. *Brady,* 740 F. Supp. 1007, 1015 (S.D.N.Y. 1990). Similarly, the 1994 amendment codified the decision in *Cernuda* v. *Heavey,* 720 F. Supp. 1544, 1548 (S.D. Fla. 1989), by adding ''artworks'' to the illustrative list of informational materials and otherwise took the opportunity to ''expand[ ] the exemption's non-exclusive list of informational materials to include new media, such as compact discs and CD ROMs,'' on which expressive information may exist.[371] But the House conference report makes clear that the 1994 amendment ''only intended to address some of those restrictive interpretations'' while leaving other interpretations in place.[372] For example, Congress ''did not disabuse OFAC of its belief that it could permissibly regulate 'informational materials not fully created and in existence at the date of the transaction' '' and ''did not counteract'' that interpretation, which is discussed in more detail below.[373] By explicitly acknowledging that the bill was intended to overrule some but not all narrow interpretations of ''information or informational materials,'' Congress rejected a meaning that would include anything that, in a colloquial sense, could potentially be ''information or informational materials.'' [374]

Similarly, Rep. Howard Berman, the sponsor of the original Berman Amendment in 1988, described the 1994 amendment as designed to protect the right ''to impart and receive information and ideas.'' [375] ''Even at the height of the Cold War,'' he recounted, the United States ''positively promoted the exchange of literary and artistic work in an attempt to liberalize and open up the cultural and political climate in those countries,'' and the then-recent fall of the Soviet Union ''suggest[ed] that contact with Americans and the exposure to American ideas were crucial to the momentous changes which are taking place there, to our great national advantage.'' [376] The legislative history underscores what is apparent in the statutory text and context: The term is not meant to encompass everything that might technically or colloquially be described as ''information.''

Congress' purpose in enacting the Berman Amendment was to protect the free exchange of ideas, and the Berman Amendment does not exempt from regulation all types of conduct, information, or communications.[377] Although the message need not be particularized or articulable, as in the case of many pieces of art, it must still ''communicate . . . ideas.'' [378] The types of ''information or informational materials'' listed in the Berman Amendment, such as ''publications,'' ''news wire feeds,'' and ''artworks,'' are mediums for expressing and conveying an idea to others.[379]

B. Regulated Transactions Involving Sensitive Personal Data Under This Proposed Rule Do Not Implicate the Berman Amendment's Restrictions on Regulating Expressive Material

The proposed rule would regulate transactions involving sensitive personal data that is non-expressive and thus is fully consistent with the Berman Amendment.[380] It would regulate commercial transactions involving the export of government-related data or bulk U.S. sensitive personal data that lacks expressive content.

The specific types of sensitive personal data proposed here for regulation are not expressive in nature because the data itself, whether in bulk or in isolation, does not convey an idea.[381] For example, a person's fingerprints (biometric identifiers); DNA sequence (genomic data); financial account numbers or their browser's IP address (covered personal identifiers); debts and income (personal financial data); weight, blood type, test results, and treatments (personal health data); and their telephone's location history (precise geolocation data) do not convey expressive messages or ideas to the recipient. Sensitive personal data instead serves functional purposes, and the regulations proposed here are designed to prevent the export of this data based on its functionality to create and facilitate national security harms, not regulate the expression of ideas.

For example, human genomic data is the biological code of human functioning and growth. It is primarily used (along with personal health data)

[366] *See Cernuda,* 720 F. Supp. at 1549–52.

[367] H.R. Rep. No. 103–482, 103d Cong., 2d Sess., at 239 (conf. rep.), reprinted in 1994 U.S.C.C.A.N. 398, 483; *see* Public Law 103–236, sec. 525(b), 108 Stat. 382, 474 (1994) (codified at 50 U.S.C. 1702(b)).

[368] Public Law 103–236, *supra* note 367, at 474.

[369] *Id.*

[370] H.R. Rep. No. 103–482, *supra* note 367, at 239.

[371] *Kalantari* v. *NITV, Inc.,* 352 F.3d 1202, 1205 (9th Cir. 2003).

[372] H.R. Rep. No. 103–482, *supra* note 367, at 239.

[373] *United States* v. *Amirnazmi,* 645 F.3d 564, 586 (3d Cir. 2011).

[374] *See, e.g., id.* at 586–87 (''When Congress is aware of an agency's interpretation of a statute and takes no action to correct it while amending other portions of the statute, it may be inferred that the agency's interpretation is consistent with congressional intent.'').

[375] 138 Cong. Rec. 15052 (June 16, 1992) (statement of Rep. Berman).

[376] *Id.*

[377] *See, e.g., Texas* v. *Johnson,* 491 U.S. 397, 404 (1989).

[378] *Hurley* v. *Irish-Am. Gay, Lesbian & Bisexual Grp. of Bos.,* 515 U.S. 557, 570 (1995).

[379] 50 U.S.C. 1702(b)(3).

[380] *See infra* §§ 202.249(b)(4) (excluding from the definition of ''sensitive personal data'' ''information or informational materials''), 202.226(a) (limiting ''information or informational materials'' to ''expressive materials'').

[381] So too for ''government-related data,'' which the proposed rule defines to mean certain sensitive personal data or certain precise geolocation data, regardless of volume.

to understand and address vulnerabilities in human functioning, health, and disease. The same human genomic data that can be used to design disease therapy can also be used to identify genetic variability in a population, which can potentially be used for nefarious purposes such as identifying and exploiting susceptibility to disease. Large human genetic datasets used for ancestry, solving crimes, and research can also be misused for counterintelligence purposes, including targeting, surveillance, coercion, blackmail, intimidation, and influence.[382] Datasets containing human genomic data do not communicate any idea; they simply contain functionally useful data.

Biometric identifiers (like a fingerprint, palm print, iris pattern, or facial feature) are ''the measurement of physiological characteristics'' of an individual that are primarily used for security and identity verification—for example, by comparing the measurements of an identifier against those of previously enrolled identifiers permitted to access a system.[383] Similarly, precise geolocation data measures geographic location, ordinarily defined by its longitude and latitude coordinates, that is used to identify the physical location of a device (and thus persons associated with the device). Geolocation data is primarily used to enable and facilitate, for example, navigation, tracking, the implementation of security measures through geofencing, anti-fraud measures, targeted advertising, and the provision of certain services like roadside assistance. Biometric identifiers and precise geolocation data do not communicate any idea; they simply contain functionally useful data.

At their core, and as defined in these proposed regulations, personal financial data and personal health data also contain only functionally useful data that does not convey any idea or message. The former typically identifies and measures an individual's financial accounts, assets, debts, and liabilities, primarily to enable, facilitate, and track commercial activity (for example, by exchanging account and routing numbers, balances, and amounts to enable payments, or by identifying assets, debts, and liabilities associated with a particular individual to determine creditworthiness for loan applications). The latter typically identifies and measures an individual's medical conditions and history, primarily to assess and track an individual's health condition and determine a medical course of action.

Finally, covered personal identifiers are specifically listed classes and combinations of data that are ''reasonably linked to an individual.'' [384] This data (such as Social Security numbers, financial account numbers, hardware-based identifiers, advertising identifiers, and network-based identifiers) is primarily used to identify devices and individuals, and to distinguish them from each other. They are not typically used to express and communicate ideas or messages.

In sum, the regulations contained in this proposed rule appropriately ''balance[ ] IEEPA's competing purposes'' in ''restricting material support for hostile regimes while encouraging the robust interchange of information.'' [385] The export of non-expressive data (including the sensitive personal data that the proposed rule would regulate) does not implicate the exchange of ideas and expression that the Berman Amendment protects. At the same time, allowing sensitive personal data to fall into the hands of countries of concern would directly support and enable their attempts to undermine national security, including through traditional and economic espionage, surveillance, sabotage, blackmail, and other nefarious activities. Moreover, these categories of sensitive personal data are already subject to some existing government regulation in the context of domestic commercial transactions. It would be unreasonable to interpret IEEPA—a statute that is specifically designed to address foreign threats to national security, foreign policy, and the economy—as disallowing regulation of the same commercial transactions when they involve transferring such data to a country of concern.

This proposed interpretation aligns with the suggestions of several commenters to clarify the extent to which the transmission of expressive content and associated metadata, including through internet traffic, to entities and individuals in countries of concern would be exempt from the proposed regulations. Under this interpretation, expressive content and associated metadata that is not sensitive personal data would be categorically outside the scope of the proposed definition of ''sensitive personal data'' and thus outside the scope of the proposed regulations, regardless of the type of activity (or transaction) involved. The Department believes that other aspects of the proposed rule (such as bulk thresholds or the definition of ''covered data transaction'') would also protect the dissemination of expressive content and its associated metadata. The Department welcomes further comments on this issue.

To the extent that any parties believe that the sensitive personal data involved in their covered data transactions may nevertheless qualify as ''information or informational materials'' that is exempt under 50 U.S.C. 1702(b)(3), they can seek clarification using the proposed administrative processes for seeking an advisory opinion or applying for a specific license before engaging in the transaction.

C. Exclusion for Materials Already Created and in Existence

Finally, consistent with longstanding OFAC practice, the proposed rule would exclude ''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'' from the definition of ''information or informational materials.'' § 202.206(b)(1). Many commercial services and transactions may result in the creation of information or informational materials. This exclusion balances ''IEEPA's competing imperatives (*i.e.,* restricting material support for hostile regimes while encouraging the robust interchange of information)'' and reflects a ''reasoned determination'' that 50 U.S.C. 1702(b)(3) is not meant to exempt ''information or informational materials'' that ''would not be produced but for'' commercial transactions that could be otherwise prohibited or regulated.[386] In the sanctions context, for example, a prohibition on providing consulting services would preclude provision of a consulting report even though such a report might otherwise be characterized as ''informational materials.'' [387] In the

[382] *See, e.g.,* Nat'l Counterintel. & Sec. Ctr., *supra* note 83, at 4.

[383] Nat'l Inst. of Standards & Tech., *Biometrics, https://www.nist.gov/programs-projects/biometrics* [*https://perma.cc/SV3S-THLD*].

[384] 89 FR 15428–29.

[385] *United States* v. *Amirnazmi,* 645 F.3d 564, 587 (3d Cir. 2011).

[386] *Amirnazmi,* 645 F.3d at 587; *see also, e.g., United States* v. *Griffith,* 515 F. Supp. 3d 106, 116–17 (S.D.N.Y. 2021).

[387] *Cf., e.g.,* Off. of Foreign Assets Control, U.S. Dep't of Treas., *Guidance on Certain Publishing Activities,* at 2–3 (Oct. 28, 2016), *https://ofac.treasury.gov/media/6516/download?inline* [*https://perma.cc/GF9U-M4TJ*]; Off. of Foreign

Continued

context of this proposed rulemaking, a U.S. company's customization and sale of bulk U.S. sensitive personal data in response to a customer's particular criteria would fall within this independent exclusion and would not constitute information or informational materials (in addition to falling outside the definition of ''information or informational material'' because it is non-expressive material).

The legislative history of the Berman Amendment indicates that Congress was aware of this same interpretation in sanctions programs under IEEPA administered by OFAC and chose not to change it. The Department of the Treasury construed the Berman Amendment not to apply to ''informational materials not fully created and in existence at the date of the transaction, or to the substantive or artistic alteration or enhancement of informational materials, or to the provision of marketing and business consulting services'' shortly after it was enacted.[388] As discussed above, when Congress amended the statute in 1994, it overrode other government interpretations of the Berman Amendment but it ''did not disabuse OFAC of its belief that it could permissibly regulate 'informational materials not fully created and in existence at the date of the transaction' '' and ''did not counteract'' that interpretation.[389] Courts, relying in part on this legislative history, have affirmed this interpretation of the Berman Amendment,[390] and the Department accordingly incorporates it into the definition of ''information or informational materials'' in proposed § 202.226.

VII. Regulatory Requirements

The Department designated the proposed rule as significant under Executive Order 12866, as amended, and the Office of Information and Regulatory Affairs in the Office of Management and Budget (''OMB'') reviewed the proposed rule.[391] In addition, this section includes the required assessments of the reporting and recordkeeping burdens under the Paperwork Reduction Act of 1995,[392] and the potential impact on small entities pursuant to the Regulatory Flexibility Act.[393]

A. Executive Orders 12866 (Regulatory Planning and Review) as Amended by Executive Orders 13563 (Improving Regulation and Regulatory Review) and 14094 (Modernizing Regulatory Review)

1. Executive Summary

The Department of Justice estimates the discounted annualized cost of the proposed regulation to be approximately $502 million annually. The extremely high potential net benefits (*i.e.,* expected benefits less estimated costs) justify moving forward with the proposed rule. The approximately $502 million estimated annual cost would afford protection to well over 100 million American individuals who are potential targets of adversaries using bulk U.S. sensitive personal data. Also, the approximately $502 million estimated annual cost of the regulation is about one-third of 1 percent (0.3 percent) of the $176 billion revenues generated in the U.S. Computing, Infrastructure, Data Processing Services, and Web Hosting Services industry sector.

2. Introduction.

The review that accompanies an NPRM is known as a Preliminary Regulatory Impact Analysis (''RIA''). The Office of Management and Budget's Circular A–4 provides guidance to Executive agencies on how to conduct effective regulatory analyses.[394] Circular A–4 recognizes that good regulatory analyses cannot be conducted according to a formula; that conducting high-quality analysis requires competent professional judgment; and that different regulations may call for different emphases in the analysis, depending on the nature and complexity of the regulatory issue and the sensitivity of the benefit and cost estimates of the key assumptions.[395]

Circular A–4 states that RIA analysts ''should aim for transparency about the key methods, data, and other analytical choices you make in your analysis.'' [396] It also encourages consultation with key stakeholders, which can ''be useful in ensuring that your analysis addresses all of the relevant issues and that you have access to all pertinent data,'' noting that ''[e]arly consultation can be especially helpful.'' [397] At the outset of this research, the Department reached out to the private sector and other government agencies regarding data that would be useful to the analysis. The response has, in general, been that the information and data available to and known by other agencies and the private sector that would potentially be relevant to conducting such an analysis are incomplete, irrelevant, and unreliable. The Department's own search found that there are enough information sources available to make a reasonable estimate of the impact of the proposed rule based on a cost analysis that considers the value of transactions lost due to the prohibitions, the security and due diligence costs associated with the pursuit of restricted transactions, and adequate data to approximate the number of firms likely to be affected by the regulation. Regarding the estimated value of transactions lost to the prohibitions, impacts could vary by the bulk thresholds for each of the data categories outlined in the proposed rule. However, due to data limitations, this analysis does not attempt to estimate cost sensitivities based upon alternatives to the proposed bulk thresholds. We welcome comments on addressing this analytical issue.

Given the limitations on available information, the resulting uncertainty, and the qualifications surrounding the analysis, the Department has been unable to assess that any secondary impacts, such as how the prohibition on bulk U.S. sensitive personal data transfers to the countries of concern would influence international trade, are reasonably likely. Based on the available information, such secondary impacts are too speculative and hypothetical to be

Assets Control, U.S. Dep't of Treas., Letter No. 031211–FARCL–IA–14, *Interpretive Ruling: Posting of Information from Iran on Website,* at 2 (Dec. 11, 2003), *https://ofac.treasury.gov/media/7921/download?inline* [*https://perma.cc/J7FP-CVAS*].

[388] 31 CFR 500.206(c) (1989).

[389] *Amirnazmi,* 645 F.3d at 586.

[390] *See Amirnazmi,* 645 F.3d at 583–88; *Griffith,* 515 F. Supp. 3d at 116–17.

[391] E.O. 12866, 58 FR 51735 (Sept. 30, 1993).

[392] 44 U.S.C. 3501 *et seq.*

[393] 5 U.S.C. 601 *et seq.* This proposed rulemaking pertains to a foreign affairs function of the United States and therefore is not subject to the notice-and-comment rulemaking requirements of the Administrative Procedure Act (''APA''), which exempts a rulemaking from such requirements ''to the extent there is involved . . . a military or foreign affairs function of the United States.'' 5 U.S.C. 552(a)(1). The proposed rule is being issued to assist in addressing the national emergency declared by the President with respect to the threat posed to U.S. national security and foreign policy by the continuing effort of countries of concern to access and exploit government-related data or Americans' bulk U.S. sensitive personal data. As described in the Order, this threat to the national security and foreign policy of the United States has its source in whole or substantial part outside the United States. Accordingly, the proposed rule would have a direct impact on foreign affairs concerns, which include the protection of national security against external threats (for example, prohibiting or restricting transactions that pose an unacceptable risk of giving countries of concern or covered persons access to bulk sensitive personal data). Although the proposed rule is not subject to the APA's notice and comment requirements, the Department is engaging in notice and comment rulemaking for this proposed rule, consistent with sections 2(a) and 2(c) of the Order.

[394] Off. of Mgmt. & Budget, Circular No. A–4, *Regulatory Analysis* (Nov. 9, 2023), *https://www.whitehouse.gov/wp-content/uploads/2023/11/CircularA-4.pdf* [*https://perma.cc/8J6A-K75Y*].

[395] *Id.* at 4.

[396] *Id.*

[397] *Id.*

quantified in this analysis. Although the scope of the proposed rule is limited, indirect trade impacts could run into the hundreds of millions of dollars; nevertheless, such costs would be impossible to calculate at this juncture, and such analysis is outside the scope of this assessment.

This analysis considers the direct costs of the proposed regulation. Although it does not devote a section to indirect costs, Circular A–4 advises analysts to look beyond the obvious costs and benefits of a regulation for additional costs and benefits, which are sometimes referred to as ''indirect'' effects or ''downstream'' effects.[398] Beyond the direct costs, there will be other market repercussions associated with the proposed regulation. Foreign firms will have less revenue from selling bulk U.S. sensitive personal data purchased from U.S. firms; new businesses may arise to provide vetting information to firms seeking entrance into the restricted transactions market; misunderstandings of the proposed regulation may result in firms spending more than necessary to comply; overall increased data security may result in more secure data and systems; transactions that are not prohibited may be reduced by firms not understanding nuances of the prohibitions; and, in retaliation, foreign countries may enact their own prohibitions and restrictions that may adversely affect U.S. businesses.

Additionally, staff of the Department of Commerce Office of Undersecretary for Economic Affairs note that there will be indirect costs from the loss of database imports from countries of concern, forgone productivity gains associated with potential innovation resulting from access to restricted data by individuals in countries of concern, and firms' reduced access to employees from countries of concern. At this point, the Department is not aware of any data with which to assess these costs, and the assessment of such costs is outside the scope of this RIA.

The regulatory review faces significant challenges in developing quantitative estimates of the monetary costs and benefits of the proposed regulation. Among these challenges to a reliable comparison of quantified cost and benefits, is the nature of the benefits that are expected from the regulation. These benefits include the security of the American people, economic prosperity and opportunity, and democratic values, all of which are beyond a reasonable, reliable, and acceptable estimate of quantified monetary value.[399] In contrast, although precise, reliable, and relevant data to estimate the regulation's cost impacts are not publicly available, the Department has made a preliminary estimate of those costs using knowledge of the entities affected by the proposed rule; the transactions likely to be involved; and previous estimates of the costs of compliance with similar activities, such as due diligence, audits, recordkeeping, and reporting. Policy decisions will be informed by whether the benefits expected from the regulation justify the estimated costs.

3. Market Sectors Impacted by the Proposed Regulation

The firms that are currently active in the collection, processing, sale, or other types of transfers of bulk U.S. sensitive personal data and that are likely to be impacted by the proposed regulation include those that collect sensitive personal data (often referred to as ''first parties'') and those that aggregate, assemble, analyze, and sell sensitive personal data (''third parties''). Sensitive personal data passes through a long supply chain of third-party vendors, such as data brokers, that obtain the data from first-party sources such as doctors, hospitals, pharmacies, banks and other financial companies, insurance companies, internet service providers, online and brick-and-mortar retail chains, schools, ''smart product'' sellers, rental agencies, ancestry agencies, software vendors, geolocation firms, and gaming firms.[400] Another sector that may be impacted consists of those firms that export bulk biospecimens such as blood plasma and other medical products, laboratory supplies, and cosmetic products made with human hair. The United States supplies 70 percent of the world's supply of blood plasma, for example, making it the largest exporter of blood plasma.[401] Additionally, blood plasma has become the United States' 11th most valuable export.[402] In 2022, China imported more U.S. exports of ''immunological medicines, plasma and other blood fractions'' than any other country had in a given year.[403] When it comes to the biospecimen segment, the proposed rule exempts items related to clinical trials, and official United States Government business and transactions required or authorized by international agreements, including United States Government business and international agreements related to pandemic preparedness and surveillance.

Bulk personal data that is extracted from different sources and then combined and analyzed can provide comprehensive profiles of individuals. Comprehensive profiles typically include a wide range of personal data, including contact information such as address, phone number, and email address; demographic data, including age, family ties, and ethnic and religious affiliations; data on general interests, such as charitable giving, gambling, pets, preferred celebrities, movies and music genres, and reading preferences; data about a person's home and neighborhood, including home equity, home size (*e.g.,* number of rooms and baths), and rent or loan amount and interest rate; criminal and civil actions

[398] *Id.* at 56. The usage of the term ''indirect costs'' in this analysis differs from the ANPRM's ''Economic Impact,'' which discussed the expected ''indirect costs'' of the rulemaking primarily in terms of due diligence and security costs. *See* 89 FR 15799–800. In this analysis, the term ''indirect costs'' refers to downstream effects and does not necessarily encompass due diligence and security costs; to the extent that such costs are discussed, the Department simply refers to them by their own terms.

[399] Exec. Off. of the President, *National Security Strategy* (Oct. 12, 2022), *https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-Nationalsecurity-Strategy-10.2022.pdf* [*https://perma.cc/6X6U-75DL*].

[400] *See, e.g., Types of Sensitive Information: A Complete Guide,* SealPath, *https://www.sealpath.com/blog/types-of-sensitive-information-guide/* [*https://perma.cc/7XPU-TLB6*]; Nirmal Ranganathan, *Understanding the Complexities of Enterprise Data Supply Chains,* TechRadar Pro (May 1, 2023), *https://www.techradar.com/opinion/understanding-the-complexities-of-enterprise-data-supply-chains* [*https://perma.cc/AKZ4-UJAE*]; Lou Rabon, *Uncovering Third-Party Risk: What Are They and Where They Come From,* Cyber Defense Group (June 3, 2024), *https://www.cdg.io/blog/third-party-risk* [*https://perma.cc/645V-YUBF*]. This assessment has also considered whether the proposed rule would result in a reasonably measurable impact on product development and testing. Although some commenters raised concern about such potential impacts, none of the comments were specific enough to identify any concrete product development and testing involving prohibited or restricted transactions. The comments did not describe any specific scenarios in which government-related data or bulk U.S. sensitive personal data are critical to the development or testing of some product with a significant market the proposed rule would eliminate, for example, because there is no substitute development or testing market other than a country of concern or covered person.

[401] David Smith, *'It's gamified': Inside America's Blood Plasma Donation Industry,* The Guardian (Mar. 2, 2023), *https://www.theguardian.com/books/2023/mar/02/blood-money-book-kathleen-mclaughlin* [*https://perma.cc/7VFK-QTSL*].

[402] Peter Jaworski, *Bloody Well Pay Them: The Case for Voluntary Remunerated Plasma Collections,* Niskanen Center (June 14, 2020), *https://www.niskanencenter.org/bloody-well-pay-them-the-case-for-voluntary-remunerated-plasma-collections/* [*https://perma.cc/WVR9-ZGS9*].

[403] Ken Roberts, *In 2022, China Dominates U.S. Exports of Immunological Drugs, Plasma and Vaccines,* Forbes (Oct. 26, 2022), *https://www.forbes.com/sites/kenroberts/2022/10/26/in-2022-china-now-dominates-us-exports-of-plasma-and-vaccines/* [*https://perma.cc/X9KA-EG82*].

background data, such as arrests and convictions, and judgments in civil cases; social media and technology data, including home internet provider, social media usage, and computer operating systems; financial data, including credit card usage, loans, and net worth; health data, including alcohol or tobacco usage, medical conditions (*e.g.,* allergies), medicine preferences, and mental health issues; and other data, such as travel, vehicle, and behavior data.[404]

a. Sensitive Personal Data and Government-Related Data

i. Personal Financial Data

The universe of financial institutions that create bulk U.S. sensitive personal data is all firms that provide financial services. The smallest, narrowest set is the financial firms subject to a primary financial regulator. These include banks,[405] credit unions,[406] large financial utilities,[407] securities firms,[408] investment companies,[409] and insurance companies.[410] The total number of government-regulated and -supervised financial-services firms in this category is around 35,000.[411] The total number of large financial-services firms is about 17,000. The Department arrived at this number by consulting the North American Industry Classification System (''NAICS''), which, in its category for Finance and Insurance companies, contains the broadest potential set of firms that could be found in the NAICS category for Finance and Insurance companies. This category contains more than 240,000 firms in total, with around 17,000 of these firms having over 20 employees, making them potentially more likely to have in-house data management and control systems.[412]

ii. Personal Health Data

As with human genomic data,[413] many doctors, hospitals, medical facilities, consumer human genetic testing labs, insurance companies, businesses, healthcare providers, and research institutions sell sensitive health-related data (*e.g.,* Electronic Medical Records (''EMRs''), prescriptions, laboratory tests, insurance claims). There is a large market for such data, which generates significant profits for companies with the capabilities to collect, anonymize, collate, and sell the data to third parties and data brokers. The market for these sales is at least in the billions of dollars.[414] With the EMR market expected to grow at a compound annual growth rate of 6.5 percent to $46.96 billion in 2028, it is expected that the keepers of this data will take advantage of the increasing demand and massive economic benefits that these data sales can achieve.[415]

At the forefront of data sales are the hospitals, medical facilities, pharmaceutical companies, insurers, and pharmacies that have direct access and involvement in the creation and maintenance of patient health data. HIPAA and other privacy laws help protect patients from having their personal health information shared, but nearly every State either recognizes medical providers as the owners of medical data or does not have any laws conferring patients specific ownership or property rights to their medical records.[416] The situation with clinical trial data is similar, as any data generated by a trial participant becomes the property of the sponsor company.[417]

Furthermore, some companies in the health sector may be able to legally sell Americans' health-related information, depending on the legal requirements applicable to their context.[418] For example, although healthcare providers that conduct certain standard transactions electronically may be HIPAA-covered entities that are generally prohibited from selling protected health information by the HIPAA Privacy Rule,[419] many companies that collect healthcare information are not covered by HIPAA and are not subject to its restrictions. Pairing Americans' health-related information with publicly available health record databases, healthcare directories and clearinghouses, academic or government databases (*e.g., data.gov*), and basic internet searches makes it increasingly simple to re-identify or link information. Data brokers have flourished by selling packaged datasets on the sensitive health conditions of millions of Americans in the open market.[420] As the volume and demand for this data increase, we may see continued growth in the market share.

We also note that the Department of Health & Human Services (''HHS'') is supporting the secure sharing of clinical information via the development of the voluntary Trusted Exchange Framework and Common Agreement.[421]

iii. Precise Geolocation Data

The proposed rule defines ''precise geolocation data'' as ''data, whether real-time or historical, that identifies the

[404] Urbano Reviglio, *The Untamed and Discreet Role of Data Brokers in Surveillance Capitalism: A Transnational and Interdisciplinary Overview,* 11 Internet Pol'y Rev. (Issue) 3 (Aug. 4, 2022), *https://policyreview.info/articles/analysis/untamed-and-discreet-role-data-brokers-surveillance-capitalism-transnational-and* [*https://perma.cc/A4NS-AF5B*].

[405] Bd. of Governors of the Fed. Rsrv. Sys., *110th Annual Report of the Board of Governors of the Federal Reserve System* 26–28 (2023), *https://www.federalreserve.gov/publications/files/2023-annual-report.pdf* [*https://perma.cc/3W34-QKYE*].

[406] Press Release, Nat'l Credit Union Admin., *Credit Union Assets, Lending, Insured Shares, Delinquencies Grow* (June 2024), *https://ncua.gov/newsroom/press-release/2024/credit-union-assets-lending-insured-shares-delinquencies-grow* [*https://perma.cc/MK9Z-7R3Z*].

[407] Bd. of Governors of the Fed. Rsrv. Sys., supra note 405.

[408] Fin. Indus. Regul. Auth., *2024 FINRA Industry Snapshot* 13 (July 18, 2024), *https://www.finra.org/sites/default/files/2024-07/2024-Industry-Snapshot.pdf* [*https://perma.cc/UEV6-9XVM*].

[409] Inv. Co. Inst., *2024 Investment Company Fact Book* 23 (2024) *https://www.ici.org/system/files/2024-05/2024-factbook.pdf* [*https://perma.cc/5CJ3-JWHS*].

[410] Ron Harden, *Insurance Industry Facts,* Nat'l Ass'n of Ins. Pros., Inc., *https://thenaip.org/general/insurance-industry-facts/* [*https://perma.cc/U8S9-BVRD*].

[411] This figure includes 3,794 bank holding companies; 1,411 Federal Reserve System member banks; 287 savings and loan holding companies; 8 financial market utilities; 4,572 credit unions; 3,298 securities firms; 16,038 investment companies; and 5,929 insurance entities.

[412] U.S. Census Bureau, *U.S. & states, 6-digit NAICS,* 2021 SUSB Annual Data Tables by Establishment Industry (Dec. 2023), *https://www.census.gov/data/tables/2021/econ/susb/2021-susb-annual.html* [*https://perma.cc/A86S-NKHA*].

[413] While the NPRM proposes including human 'omic data beyond genomic data within the scope of the categories of sensitive personal data, the NPRM seeks comments on how that category of human 'omic data (other than genomic data) should be regulated. The Department defers consideration of that issue until it is settled in the final rule. Section 7(i) of the Order defines human 'omic data as ''data generated from humans that characterizes or quantifies human biological molecule(s), such as human genomic data, epigenomic data, proteomic data, transcriptomic data, microbiomic data, or metabolomic data, as further defined by regulations issued by the Attorney General pursuant to section 2 of this order, which may be informed by the report described in section 6 of this order.'' E.O. 14117, 89 FR 15429.

[414] Adam Tanner, *Our Bodies, Our Data: How Companies Make Billions Selling Our Medical Records* (2017).

[415] *Electronic Medical Records Market to Surpass $46.96 Billion by 2028, Lead [sic] by Asia-Pacific Growth and AI Trends,* Yahoo! Finance (Mar. 11, 2024), *https://finance.yahoo.com/news/electronic-medical-records-market-surpass-192000251.html* [*https://perma.cc/N45N-N5QV*].

[416] Niam Yaraghi, *Who Should Profit from the Sale of Patient Data?* Brookings Inst. (Nov. 19, 2018), *https://www.brookings.edu/articles/who-should-profit-from-the-sale-of-patient-data/* [*https://perma.cc/9886-AS93*].

[417] Paul W. Glimcher, *Who Profits from Medical Records*?, Med. Econ. Oct. 2020, at 50, *available at https://www.medicaleconomics.com/view/who-profits-from-medical-records-* [*https://perma.cc/RP4S-GGZR*].

[418] Justin Sherman, *Your Health Data Might Be for Sale,* Slate (June 22, 2022), *https://slate.com/technology/2022/06/health-data-brokers-privacy.html* [*https://perma.cc/39CR-4ZS3*].

[419] *See* 45 CFR 164.502(a)(5)(ii), 164.508(a)(4).

[420] Sherman, *supra* note 418.

[421] Notice of Publication of Common Agreement for Nationwide Health Information Interoperability (Common Agreement) Version 2.0, 89 FR 35107 (May 1, 2024).

physical location of an individual or a device with a precision of within one kilometer.'' The parameters to be determined are (1) the level at which to set this precision, (2) the level of precision necessary to support common commercial applications of geolocation data, and (3) the effectiveness of applying location fuzzing to geolocation data (decreasing its accuracy) in some commercial applications to reduce potential privacy impacts. These parameters are necessary to provide clear guidance to acquirers and sellers of precise geolocation data.

Mobile applications (''apps'') from smartphones are the primary sources that directly gather location data from consumers, although other technologies are also collecting and transmitting data, such as ''Internet of Things'' wearable devices and connected vehicles. Once they collect it, many apps share location data with third parties, whether by selling it to data brokers, to advertisers who then sell it to data brokers, or directly to buyers who intend to use the geolocation data.[422] Data brokers can ''pay a mobile app developer to use the broker's software development kit . . . in the developer's app. The broker can then sit within the app and gather data directly on users.'' Alternatively, many app developers will sell location data ''directly to a data broker through a server-to-server transfer.'' [423] As one example, the family safety app Life360 sold location data to nearly a dozen location data brokers in 2021—and in fact, it had agreements to directly transfer location data about its users to data brokers through its own servers.[424] Such practices create opportunities for countries of concern to exert malign influence over U.S. persons relevant to national security.

The market for location data is large, and many companies operate as data brokers.[425] Significantly, three major data brokers—Acxiom, LexisNexis, and Nielsen—sell data on current or former U.S. military personnel, some of which is specifically marketed as such.[426] All three firms collect and advertise information on individuals, ranging from their family members and friends to their spending habits, mental health conditions, and geolocation.[427] Both Acxiom and LexisNexis also provide users with the ability to verify whether someone is active duty.[428]

iv. Human Genomic and Human 'Omic Data

There is value in both human genomic and 'omic data, and there is a large global ecosystem for buying and selling this data for a variety of purposes. The 'omic data market is growing exponentially due to the use of such data for drug discovery. There is little current regulation that restricts the buying and selling of this data, but there are real risks and potential harms associated with the misuse of such data, ranging from the individual to the population level.

The human genomic data ecosystem is large and has both public and private actors, including healthcare entities, law enforcement, international security agencies, and recreational personal human genomics/biospecimen companies.[429] The global human genomics market was valued at $28 billion in 2022 and is projected to grow to over $164 billion by 2032, with North America accounting for approximately 45 percent of the market's current size.[430]

Personal human genomics companies (*e.g.,* 23andMe, Ancestry, Ariosa Diagnostics, Color Genomics, FamilyTreeDNA, Ionis, GenScript, Illumina, Genentech, My Heritage, Navigenics, Orig3n, and Prenetics) and human biospecimen (*e.g.,* BioChain Institute, BioIVT, Boca Biologistics, Creative Bioarray, Cureline, Discovery Life Sciences, Infinity BiologiX, Precision for Medicine) companies collect human genomic and related data or human biospecimens, such as tissue and blood samples, that can be used to extract human genomic information for a variety of healthcare and recreational purposes.[431] It is common for companies in these spaces, especially direct-to-consumer firms, to be owned by pharmaceutical companies or to sell the human genomic data they obtain to pharmaceutical companies. It is also common for them to conduct health research in collaboration with healthcare systems and to enter into partnerships with other industries.[432]

There is little readily available information on who is purchasing or reselling human genomic data beyond pharmaceutical companies. Similarly, there is little readily available information on which entities (such as multinational pharmaceutical companies) are transferring human genomic data to their subsidiaries or vendors in countries of concern.

While many of the uses of human genomic data are for the development of new health technologies and pharmaceuticals, and the health and drug discovery environment are highly regulated, the sale of the data appears common and is currently virtually unregulated. As a result, there are few records of current transactions, and any company that collects human genomic data could potentially broker its sale to other companies or interested parties. For example, the States of Vermont and California have data broker registration laws, but even in those States, there is

[422] *The Location Data Market, Data Brokers, and Threats to Americans' Freedoms, Privacy, and Safety: Hearing Before the Joint Committee on Consumer Protection and Professional Licensure,* (Mass. 2023) (written testimony of Justin Sherman, Senior Fellow and Research Lead, Data Brokerage Project, Duke Univ. Sanford Sch. of Pub. Pol'y), *https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/07/Sherman-Justin_WrittenTestimony_MA_Legislature.pdf* [*https://perma.cc/52RR-J2HY*].

[423] *Id.*

[424] Alfred Ng & Jon Keegan, *The Popular Family Safety App Life360 Is Selling Precise Location Data on Its Tens of Millions of Users,* The Markup (Dec. 6, 2021), *https://themarkup.org/privacy/2021/12/06/the-popular-family-safety-app-life360-is-selling-precise-location-data-on-its-tens-of-millions-of-user* [*https://perma.cc/NTK2-CL96*].

[425] *See The Location Data Market, Data Brokers, and Threats to Americans' Freedoms, Privacy, and Safety, supra* note 422, at 3 (listing some of the ''significant companies in the location data market'').

[426] Justin Sherman, *Data Brokers Are Advertising Data on U.S. Military Personnel,* Lawfare (Aug. 23, 2021), *https://www.lawfaremedia.org/article/data-brokers-are-advertising-data-us-military-personnel* [*https://perma.cc/Y9RN-WHZF*].

[427] Steven J. Arango, *Data Brokers Are a Threat to National Security,* Vol. 148/12/1,438 U.S. Naval Inst.: Proceedings (Dec. 2022). *https://www.usni.org/magazines/proceedings/2022/december/data-brokers-are-threat-national* security [*https://perma.cc/74W3-TCR3*].

[428] *Id.*

[429] Abraham P. Schwab et al., *Genomic Privacy,* 64 Clinical Chemistry 1696 (2018), *https://academic.oup.com/clinchem/article/64/12/1696/5608647* [*https://perma.cc/Q89R-5WRZ*].

[430] Precedence Rsch., Report No. 1204, *Genomics Market—Global Industry Analysis, Size, Share, Growth, Regional Outlook and Forecast, 2023 to 2032* (Nov. 2023), *https://www.precedenceresearch.com/genomics-market* [*https://perma.cc/J9WA-RKVB*].

[431] Susi Geiger & Nicole Gross, *A Tidal Wave of Inevitable Data? Assetization in the Consumer Genomics Testing Industry,* 60 Bus. & Soc'y 614 (2021), *https://journals.sagepub.com/doi/10.1177/0007650319826307* [*https://perma.cc/7YSC-VTEW*]; Ramish Cheema, *Top 20 Genomics Companies in the World,* Yahoo! Finance (Oct. 30, 2023), *https://finance.yahoo.com/news/top-20-genomics-companies-world-194600414.html* [*https://perma.cc/8WXD-KGCC*]; Kayte Spector-Bagdady, *Hospitals Should Act Now to Notify Patients About Research Use of Their Data and Biospecimens,* 26 Nature Med. 306 (2020), *https://www.nature.com/articles/s41591-020-0795-6* [*https://perma.cc/BEX6-3GCJ*]; InsightAce Analytic, Report No. 1264, *Biospecimen Contract Research Services Market Size, Share & Trends Analysis Report, 2024–2032* (2024), *https://www.insightaceanalytic.com/report/global-biospecimen-contract-research-services-market/1264* [*https://perma.cc/N667-TL8F*].

[432] Geiger & Gross, *supra* note 431, at 625–26, 638; Shmuel I. Becher & Andelka M. Phillips, *Data Rights and Consumer Contracts: The Case of Personal Genomic Services, in* Data Rights and Private Law 83 (Damian Clifford et al. eds., 2023), *https://ssrn.com/abstract=4180967* [*https://perma.cc/35GE-ZQQ4*].

not specific information regarding genomic information sales.[433]

v. Biometric Identifiers

The proposed rule defines biometric identifiers'' as ''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.'' In recent years, such identifiers have become increasingly ubiquitous in our security and verification systems. A wide variety of companies and agencies collect this information, amassing large datasets on everything from face shape, eye scans, and fingerprints to voice recordings and even heartbeats.[434]

There is also limited information regarding the biometric data broker community. Because of the highly sensitive nature of the data (*i.e.,* fingerprints cannot be changed), brokers are not forthcoming in their advertising or collection of available information.

vi. Covered Personal Identifiers

An individual can have personal identifiers both assigned to them and collected from them in a wide variety of contexts and through a wide variety of entities—including governments, advertisers, and providers of technology and communications services. This, combined with the fact that personal identifiers have been used in some form for many years, means that they are a widely available form of sensitive personal data. The proposed rule specifies two subcategories of covered personal identifiers that could be used, when combined with each other or combined with other types of sensitive personal data, to ''identify an individual from a data set or link data across multiple data sets to an individual.'' [435] These subcategories of covered personal identifiers in the proposed rule are listed identifiers: (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.[436] *See* § 202.212.

b. The Data-Brokerage Market

Much of the economic impact of the proposed rule's restrictions on the transfer or sale of data types described in part VII.A.3.a of this preamble will be borne by firms involved in the data-brokerage market. The United States is widely perceived to be the largest data-brokerage market in the world, as described below in this section. While the proposed rule regulates data-brokerage activities (*i.e.,* transactions), there does not appear to be any direct measure of data-brokerage activities. This analysis therefore uses and examines information regarding first-party data brokers and third-party data brokers as a reasonable measure of data-brokerage activities.

i. Companies That May Meet the Definition of Data Brokers for the Purposes of the Proposed Rule

Data brokers collect, aggregate, and sell personal data.[437] First-party or primary data brokers collect and sell information from their own customers. Third-party data brokers purchase and resell data. On the global scale, an estimated 5,000 data-brokerage firms operate worldwide.[438] There may be as many as 11,000 firms that fall under the 518210 NAICS code, which covers firms that provide data processing, hosting, and related services.[439]

ii. Market Size

Estimates of the size of the data broker market vary widely, from $50 billion to $300 billion, with one popular estimate claiming that over $200 billion in revenue is generated globally each year.[440] For the United States, which maintains approximately 60 percent of the global market, a likely range is between $30 billion and $180 billion.[441]

Based on total revenue (U.S. and foreign) and the number of employees at these firms, the Department estimates the market size as shown in Table VII–1 of this preamble.

TABLE VII–1—SELECTED DATA BROKER REVENUE AND EMPLOYEE FIGURES

Data broker	Total revenue	U.S. revenue	Foreign revenue	Employees
Acxiom (2018) [a]	$917.4 million	$834.6 million	$82.8 million	3,380
LexisNexis (2021) [b]	$974.3 million	n/a [c]	n/a [c]	10,200
Oracle America (2023) [d]	$50 billion	$31 billion	$19 billion	[g] 164,000
Equifax (2023) [e]	$5.3 billion	$4.1 billion	$1.2 billion	14,900
Experian (2022) [f]	$6.6 billion	$4.4 billion	$2.2 billion	22,000

[a] Acxiom LLC *2018 Annual Report, AnnualReports.com* (2018), *https://www.annualreports.com/HostedData/AnnualReports/PDF/NASDAQ_ACXM_2018.pdf* [*https://perma.cc/6BVA-DQS5*].

[b] Latka, *How LexisNexis Hit $974.3M Revenue with a 10.2K Person Team in 2021,* SaaS Database, *https://getlatka.com/companies/lexisnexis* [*https://perma.cc/M4DM-HAC9*].

[c] LexisNexis is owned by RELX and is folded into their annual report and therefore the annual report does not provide specific domestic and foreign revenue numbers just for LexisNexis.

[433] Both California's and Vermont's regulations provide definitions of ''Data Broker'' that differ from the definition of ''data brokerage'' provided in Subpart C of the proposed rule. *See* Cal. Civ. Code sec. 1798.99.80, *supra* note 62; Vt. Stat. Ann. tit. 9, sec. 2430(4) (2024).

[434] Samuel Chapman, *Understanding Biometric Data Collection in 2024, PrivacyJournal.net* (Apr. 10, 2023), *https://www.privacyjournal.net/biometric-data-collection/* [*https://perma.cc/RAQ2-VTLZ*].

[435] 89 FR 15428.

[436] *Id.*

[437] *How to Stop Data Brokers from Selling Your Personal Data,* Kaspersky, *https://usa.kaspersky.com/resource-center/preemptive-safety/how-to-stop-data-brokers-from-selling-your-personal-information* [*https://perma.cc/ZLU3-S7N9*].

[438] Susan Moore, *How to Choose a Data Broker,* Gartner (June 8, 2016), *https://www.gartner.com/smarterwithgartner/how-to-choose-a-data-broker* [*https://perma.cc/5FP2-RGM5*].

[439] U.S. Census Bureau, *supra* note 412.

[440] *How Data Brokers Sell Your Identity & Personal Information,* IDShield: Blog (Mar. 18, 2022), *https://www.idshield.com/blog/internet-privacy/data-brokers-what-they-know-and-how-they-collect-your-data/* [*https://perma.cc/6LRX-SX79*]; Catherine Tucker & Nico Neumann, *Buying Consumer Data? Tread Carefully,* Harv. Bus. Rev. (May 1, 2020), *https://hbr.org/2020/05/buying-consumer-data-tread-carefully* [*https://perma.cc/GDY3-AWKQ*]; David Lazarus, *Shadowy Data Brokers Make the Most of Their Invisibility Cloak,* L.A. Times (Nov. 5, 2019), *https://www.latimes.com/business/story/2019-11-05/column-data-brokers* [*https://perma.cc/AH6C-UKDA*]; OnAudience.com, *Global Data Market Size: 2017–2021* (Nov. 2020), *https://pressmania.pl/wp-content/uploads/2020/12/Global-Data-Market-Size-2017-2021-OnAudience-Report.pdf* [*https://perma.cc/KX6E-4XC6*].

[441] OnAudience.com, *supra* note 440 at 8, 11.

[d] Oracle, *Oracle Announces Fiscal 2023 Fourth Quarter and Fiscal Full Year Financial Results* (June 12, 2023), *https://investor.oracle.com/investor-news/news-details/2023/Oracle-Announces-Fiscal-2023-Fourth-Quarter-and-Fiscal-Full-Year-Financial-Results/default.aspx* [*https://perma.cc/DL8Y-H2VM*]. The U.S. Revenue entry of $31 billion is for ''the America's.'' The Foreign Revenue entry of $19 billion is for ''Europe/Middle East/Africa'' and ''Asia/Pacific.'' Oracle, Culture and Inclusion Empowers Diversity, *https://www.oracle.com/careers/culture-inclusion/best-practices/* [*https://perma.cc/3M2B-GQ7F*].

[e] Equifax Inc., *2023 Annual Report* (2024), https://investor.equifax.com/sec-filings/annual-reports##document-3666-0001308179-24-000246-2 [*https://perma.cc/WU9A-NHZ2*].

[f] Experian, *Annual Report 2023* (2023), *https://www.experianplc.com/content/dam/marketing/global/plc/en/assets/documents/reports/2023/annual-report/experian_annual_report_2023_web.pdf* [*https://perma.cc/7QRT-GN3T*].

[g] Oracle Corp., Annual Report (Form 10–K) (June 20, 2023), *https://www.sec.gov/Archives/edgar/data/1341439/000095017023028914/orcl-20230531.htm* [*https://perma.cc/4ADX-R6EJ*].

iii. Products Sold by Data Brokers

Data brokers often collect data regarding, for example, where the average person goes, where they shop, and what they search for online.[442] Notably, researchers from Duke University who used a secret shopper approach were offered access to thousands of records of military personnel and military veterans' data containing names, addresses, emails, phone numbers, military agency or branch, medical ailments, political affiliations, religion, gender, age, income, credit rating, and even details on children in the household.[443] Not all brokers sell the same data, with many targeting niche industries or markets to help them gain a competitive advantage. Brokers also trade and combine their data with primary collectors to create detailed profiles they can package and commercialize.[444]

iv. Price Information

Depending on its type and volume, personal data can be purchased for prices ranging from less than $1 for one personal record to millions of dollars for a large dataset. In a secret shopper study, Duke University researchers found that they could purchase a single record for as little as $0.12 and spend upwards of $10,000 for approximately 50,000 records of service members and military veterans. The price did not noticeably vary based on the data subjects' IP location (United States vs. Singapore). The Duke University researchers found that if one broker could not sell the information to them, another one could. There are estimates that mental health datasets could range between $15,000 and $100,000 and may be sold for even higher prices if the datasets include more detailed demographic data.[445]

v. Customers of Data-Brokerage Products

It is known that data brokers sell datasets both domestically and internationally; however, specific transaction activities with these parties are difficult to ascertain from available financial reports. The U.S. Bureau of Economic Analysis (''BEA'') faces significant limitations for estimating the size of the domestic and international markets because BEA data does not break out data brokerage separately as an industry. Furthermore, based on sample financial data of the data-brokerage firms listed in Table VII–1 of this preamble, the Department estimates that the U.S. market produces over 60 percent of data broker revenue.

c. Agreements Affected by the Proposed Regulation

It is difficult to determine an approximate number of affected vendor agreements, employment agreements, and investment agreements that are entered in any given year by a U.S. person due to the scope and nature of these agreements. Each of these three types of agreements are considered restricted transactions if they involve access to government-related data or bulk U.S. sensitive personal data. The Department welcomes comments that provide a source for the annual number of vendor agreements, employment agreements, and investment agreements that might be affected by the regulation.

i. Vendor Agreements

According to the proposed rule, a vendor agreement is defined as ''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.'' *See* § 202.258(a). A potential example of a vendor agreement covered by the proposed rule is a medical facility in the United States that contracts with a company headquartered in a country of concern to provide information technology (''IT'') related services. The medical facility has bulk personal health data on its U.S. patients, and the IT services provided under the contract involve access to the medical facility's systems containing that bulk personal health data. (*See* Example 2 in § 202.258(b)). The NPRM also discusses additional examples of vendor agreements pertaining to technology services and data storage. (*See* Examples 3 and 4 in § 202.258(b)).

The costs of compliance with the security requirements will vary. Covered persons who have vendor agreements within the scope of the proposed rule may face costs associated with either replacing a vendor located in a country of concern or spending more on compliance (*e.g.,* implementing the security requirements) to maintain those vendor agreements. Furthermore, some U.S. companies may choose to remove vendor agreements altogether rather than bear the cost of complying with the security requirements. In contrast, most Fortune 500 companies or companies in sectors subject to cybersecurity regulations already have cybersecurity controls in place and might only need minor modifications to their existing vendor agreements and data security controls, while companies with less mature cybersecurity programs may require more significant changes.

ii. Employment Agreements

This NPRM defines an employment agreement as ''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.'' *See* § 202.217(a). A potential example of an employment agreement is a U.S. company that employs a team of individuals who are citizens of and primarily reside in a country of concern and have access to back-end IT services

[442] *Public Hearing on HB 2052 Before the H. Comm. On Bus. & Labor,* 82nd Leg. Assemb. (Or. 2023) (written public testimony, Or. Dep't of Just., Off. of the Att'y Gen.), *https://olis.oregonlegislature.gov/liz/2023R1/Downloads/PublicTestimonyDocument/40843* [*https://perma.cc/XVM5-4ZEJ*].

[443] Sherman et al., *supra* note 6.

[444] Henrik Twetman & Gundars Bergmanis-Korats, *Data Brokers and Security,* NATO Strategic Comm'ns Ctr. of Excellence (2021), *https://stratcomcoe.org/publications/data-brokers-and-security/17* [*https://perma.cc/XJ4D-UQYP*].

[445] Joanne Kim, *Data Brokers and the Sale of Americans' Mental Health Data* (2023) *https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/02/Kim-2023-Data-Brokers-and-the-Sale-of-Americans-Mental-Health-Data.pdf* [*https://perma.cc/48UN-ELKG*].

and company systems that contain bulk human genomic data (*see* Example 1 in § 202.217(b)). Similarly, the employment of a lead project manager or a CEO of a U.S. company who primarily resides in a country of concern and who has access to bulk U.S. sensitive personal data would be considered a restricted transaction (*see* Examples 2 and 3 in § 202.217(b)).

Any employment agreements involving government-related data or bulk U.S. sensitive personal data between U.S. persons and countries of concern or covered persons would need to comply with security requirements. The cost of security and due diligence requirements may drive some companies to cease employment agreements with these covered persons, while other companies may incur costs to ensure compliance or even implement job transfers to eliminate the potential cost of compliance with the proposed regulation. Ultimately, employment agreements may incur larger upfront costs once the proposed regulation comes into effect that may be minimized over time as the initial market disruptions due to the proposed rule settle, the costs associated with job transfers are minimized, and firms learn how to operate in the changed environment.

iii. Investment Agreements

This NPRM defines an investment agreement as ''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.'' *See* § 202.228(a). An example is when a U.S. company intends to build a data center located in a U.S. territory to store bulk personal health data on U.S. persons, and 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 (*see* Example 1 in § 202.227(c)). Ultimately, investment agreements may incur larger upfront costs once the proposed regulation comes into effect that may be minimized over time.

iv. Security Requirements

The proposed rule authorizes three classes of otherwise prohibited transactions (vendor agreements, employment agreements, and investment agreements) if they meet the security requirements proposed by CISA. The goal of the proposed security requirements is to address national security and foreign-policy threats that arise when countries of concern and covered persons access government-related data or bulk U.S. sensitive personal data that may be implicated by the categories of restricted transactions. The proposed security requirements (incorporated by reference in § 202.402 of this NPRM) have been developed by DHS through CISA, which has published the proposed requirements on its website, as announced via a **Federal Register** request for comments on the proposed security requirements, issued concurrently with this proposed rule. After CISA receives and considers public input, it will revise as appropriate and publish the security requirements.

Regarding investment agreements, as described in § 202.228 and § 202.508, the proposed rule would treat investment agreements entered into by U.S. persons with countries of concern or covered persons as restricted transactions even if they are also covered transactions subject to CFIUS review, unless and until CFIUS issues an interim order, enters into a mitigation agreement, or imposes a condition with respect to a particular covered transaction.[446] As a result, any investment agreement that is both a restricted transaction under the proposed rule and a covered transaction subject to CFIUS review would be subject to the security requirements under the proposed rule unless and until the transaction is filed with CFIUS and CFIUS takes a ''CFIUS action,'' as defined in the proposed rule, by entering into a mitigation agreement or imposing mitigation measures. Because the security requirements are likely at least similar to and potentially less burdensome than any bespoke mitigation measures that CFIUS would enter into or impose, the parties to such a covered transaction would likely face, as a result of the proposed rule, only the marginal cost of complying with the security requirements before CFIUS takes action. Because this cost of compliance is marginal, and because it appears likely, based on the Department's experience, that many investment agreements by countries of concern or covered persons that involve access to sensitive personal data would also be covered transactions subject to CFIUS review, it appears likely that there will not be a meaningful cost for investment agreements to comply with the security requirements.

v. Due Diligence and Recordkeeping

Due diligence and recordkeeping requirements will be important considerations when engaging in a restricted transaction or as a condition of a license (general or specific) and may be similar to certain requirements of an IEEPA-based sanctions program administered by OFAC. Section 202.1101 of the proposed rule requires U.S. persons subject to these affirmative requirements to maintain documentation of their due diligence to assist in inspections and enforcement, and to maintain the results of annual audits that verify their compliance with the security requirements, as applicable, and the conditions of any licenses, where relevant, that the U.S. persons may also have. Entities may be required to collect, maintain, and analyze readily available information to make appropriate judgments regarding their transactions and potential requirements under the proposed regulation. They may also be required to make available to the Department any annual audits that verify the U.S. person's compliance with the security requirements and any conditions on a license.

vi. Audits

The proposed rule imposes certain audit requirements on restricted transactions to ensure compliance with the security requirements for covered data transactions, such as appointing a qualified auditor to annually assess compliance. Such audits would address the nature of the U.S. person's covered data transaction and whether it is in accordance with applicable security requirements, the terms of any license issued by the Attorney General, or any other aspect of the regulations.

vii. Licenses

General and specific licenses would be available under the proposed regulation. Such licenses would permit transactions that are otherwise prohibited by the proposed regulation. Both general and specific licenses could include a range of requirements or obligations as the Department deems appropriate. The benefits of this type of regime include giving regulated parties the ability to bring specific concerns to the Department and seek appropriate regulatory relief and affording the Department the flexibility to resolve varied cases either generally or individually.

[446] Security requirements may only need to be implemented while the transaction is pending CFIUS review if the transaction is undertaken in the interim. *See, e.g.,* Example 9 in § 202.508.

4. Need for Regulatory Action

There are many statutes, regulations, and programs that aim to keep America secure by monitoring, restricting, prohibiting, or otherwise regulating the flow of goods, services, investments, and information to foreign countries and foreign nationals, especially countries considered to be adversaries. For example, CFIUS has the authority to take action to mitigate any national security risk arising from certain foreign investments in U.S. businesses or involving U.S. real estate, or to recommend that the President suspend or prohibit a transaction on national security grounds. In addition, OFAC ''administers and enforces economic and trade sanctions based on U.S. foreign-policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy, or economy of the United States.'' [447]

In Executive Order 13873, the President authorized the Department of Commerce to prohibit transactions in the information and communications technology and services supply chain or to impose mitigation measures to address an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.[448] The Secretary of Commerce exercises this authority through the Bureau of Industry and Security.[449] Executive Order 14034 takes various steps to protect sensitive personal data from foreign adversaries.[450]

While existing legislation provides the Department of Justice with authority to promulgate this proposed rule, no existing statute replicates the measures undertaken here. Neither do any of the previous executive actions set forth in Executive Order 14117 [451] broadly empower the government to prohibit or otherwise restrict the sale or transfer of government-related data or bulk U.S. sensitive personal data to countries of concern. Therefore, the proposed regulation will not be duplicative of any existing regulatory regime.

As relevant here, the regulatory philosophy of Executive Order 12866 provides that agencies should issue regulations when there is a compelling public need, such as a market failure.[452] Executive Order 12866 further directs agencies issuing new regulations to identify, where applicable, the specific market failure that warrants new agency action and to assess its significance. In perfect, unregulated markets, supply and demand lead to transactions that allocate resources efficiently, fully supply the market at prices that buyers are willing to pay, and do not harm third parties. However, some transactions result in market failures known as ''negative externalities;'' that is, harms to parties not directly involved in the transactions. The sale of government-related data or bulk U.S. sensitive personal data to adversaries is an example. Such transactions are mutually beneficial to the parties: U.S. data brokers obtain monetary benefits, and adversaries obtain possession of a potentially strategic asset of sensitive data that they can put to malicious use. However, when the data can be used to harm U.S. nationals who are not directly involved in the transactions by presenting a risk to national security or foreign policy, then the transaction creates negative externalities. These market failures demonstrate a need for the regulation being proposed, which will eliminate or reduce the risk to national security and foreign policy from such transactions. Circular A–4 also recognizes a common need for regulation to protect civil rights, civil liberties, or advancing democratic values, all of which are threatened if government-related data or bulk U.S. sensitive personal data end up in the hands of adversaries.[453]

5. Baseline (Without the Proposed Rule)

The baseline refers to what the world would look like without the regulatory changes being proposed here, which is closely related to the need for the regulation described above. To inform the public of the rationale behind the agency's proposed regulations, the Department must analyze the quantifiable and qualitative costs and benefits of the proposed action. The baseline for the proposal under consideration is the state of the world without the regulation, often referred to as the ''no-action alternative,'' which here includes the current regulatory regime.

a. Baseline National Security and Foreign-Policy Risks by Category of Data

i. Human Genomic and Human 'Omic Data

Human genomic data presents characteristics that, under certain circumstances, allow for misuse. Although humans share more than 99 percent of their DNA, the remaining differences play a significant role in physical and mental health.[454] In addition to genomic data, which describes a person's DNA sequence, if combined with other data, data characterizing other human systems, known as 'omic data, can also uniquely identify individuals. For example, transcriptomic data describes RNA transcripts, or the expression of genes as impacted by environmental factors; proteomic data describes the complete set of proteins expressed by a cell, tissue, or organism; and metabolomic data describes the small molecule metabolites found within a biological sample.

Human genomic data and human 'omic data are therefore highly personal, and there are both person- and population-level risks to national security associated with the potential sale of such data to foreign adversaries.[455] Genomic data has been widely acknowledged in scientific, policy, and ethics literature to have the potential to be used to track an individual; breach their privacy; and expose individuals to discrimination, exclusion, or social embarrassment when paired with other personally identifiable information, such as by coloring public perception of a person's competence or health. Genomic data that is de-identified by standard healthcare practices (*i.e.,* removal of name, date of birth) can, in some cases, be potentially re-identified by methods that combine genomic data with other privately and publicly available information.[456] There are also other

[447] U.S. Dep't of Treas., Off. of Foreign Assets Control, *https://ofac.treasury.gov/* [*https://perma.cc/4N8E-X7XM*].

[448] 84 FR 22689–22690.

[449] Office of Information and Communications Technology and Services (OICTS), Bureau of Industry and Security, *https://www.bis.gov/OICTS* [*https://perma.cc/MFX8-MDN4*].

[450] 86 FR 31423.

[451] 89 FR 15422.

[452] *See* 58 FR 51735.

[453] *See* Off. of Mgmt. & Budget, *supra* note 394, at 15.

[454] *The Human Genome Project,* Nat'l Hum. Genome Rsch. Inst., *https://www.genome.gov/human-genome-project* [*https://perma.cc/55Z4-XHFN*].

[455] Kirsty Needham, *Special Report: COVID Opens New Doors for China's Gene Giant,* Reuters (Aug. 5, 2020), *https://www.reuters.com/article/world/special-report-covid-opens-new-doors-for-chinas-gene-giant-idUSKCN2511CD/* [*https://perma.cc/U4B2-Y4TB*]; Nat'l Acads. of Scis., Eng'g & Med., *Safeguarding the Bioeconomy* 296–306 (2020), *https://nap.nationalacademies.org/catalog/25525/safeguarding-the-bioeconomys* [*https://perma.cc/77RH-ACKG*]; Bonomi et al., *supra* note 237, at 647.

[456] Adam Tanner, *Strengthening Protection of Patient Medical Data,* Century Found. (Jan. 10, 2017), *https://tcf.org/content/report/strengthening-protection-patient-medical-data/* [*https://perma.cc/R26L-G9WP*].

potential risks related to such data.[457] For instance, the 2023 Annual Threat Assessment of the U.S. Intelligence Community explains that generally, ''[r]apid advances in dual-use technology, including bioinformatics, synthetic biology, nanotechnology, and genomic editing, could enable development of novel biological weapons that complicate detection, attribution, and treatment.'' [458] Additionally, as the National Counterproliferation and Biosecurity Center has stated, ''[r]esearch in genome editing by countries with different regulatory or ethical standards than those of Western countries probably increases the risk of the creation of potentially harmful biological agents or products.'' Furthermore, because biological relatives share some genetic traits, the misuse of genomic and related information can potentially harm not only the individual but also their current and future biological relatives, to some degree.

For example, Huntington's Disease is neurodegenerative, is frequently highly incapacitating, has no cure, and is tied to specific genetic variants.[459] Revealing that an individual carries the variants for Huntington's Disease could therefore be used to claim that a political candidate for office may soon become incapacitated or to harm that person's family members mentally or emotionally.

At a population level, there are multiple examples of the risks posed by harmful use of genomic data. For example, the PRC has collected and used genetic data from minority groups and potential political dissidents to carry out human-rights abuses against those groups and to support state surveillance.[460] The PRC's collection of healthcare data from the United States poses equally serious risks, not only to the privacy of Americans, but also to the economic and national security of the United States.[461]

It is conceivable that bulk genomic data in the wrong hands could be used to identify or track ethnic or racial subgroups in the United States and to target them for physical, mental, or emotional harm. As the NCSC has publicly explained, for example, ''[c]oncerns over the exploitation of healthcare and genomic data by the [People's Republic of China] are not hypothetical,'' as China ''has a documented history of exploiting DNA for genetic surveillance and societal control of minority populations in Xinjiang, China.'' [462] Specifically, China ''has established a high-tech surveillance system across Xinjiang, as part of a province-wide apparatus of oppression aimed primarily against traditionally Muslim minority groups.'' [463] This apparatus includes an ''initiative launched by the PRC government in 2014'' that ''has been used to justify the collection of biometric data from all Xinjiang residents ages 12 to 65.'' [464] Chinese authorities have ''collected DNA samples, fingerprints, iris scans, and blood types'' and linked the biometric data ''to individuals' identification numbers and centralized [it] in a searchable database used by PRC authorities.'' [465] As NCSC has further explained, ''[s]pecific abuses by the PRC government as part of this effort include mass arbitrary detentions, severe physical and psychological abuse, forced labor, oppressive surveillance used arbitrarily or unlawfully, religious persecution, political indoctrination, and forced sterilization of members of minority groups in Xinjiang.'' [466] In 2020, the Department of Commerce ''sanctioned two subsidiaries of China's BGI for their role in conducting genetic analysis used to further the PRC government's repression of Uyghurs and other Muslim minority groups in Xinjiang.'' [467] As this example shows, ''[t]he combination of stolen PII, personal health information, and large genomic data sets collected from abroad affords the PRC''—and other countries of concern—''vast opportunities to precisely target individuals in foreign governments, private industries, or other sectors for potential surveillance, manipulation, or extortion.'' [468] The potential exploitation of this kind of data is not limited to targeting and repression within the borders of a country of concern, as this data could help ''not only recruit individuals abroad, but also act against foreign dissidents.'' [469]

There are additional risks to national security associated with the sale of bulk genomic data to countries of concern. For example, BGI Group, a Chinese company, grew exponentially during the COVID–19 pandemic by selling COVID–19 test kits in 180 countries around the world, which enabled it to collect biospecimens and DNA sequences from the individuals tested.[470] The company also built laboratories in 18 countries, widely distributing its genetic sequencing/gathering technology across the globe, and the government of China helped to coordinate some of BGI's arrangements with other countries. The human genetic samples that BGI collected may be shared publicly on China's government-funded National GeneBank, creating individual privacy risks, and the Chinese government has indicated that its backing of BGI is intended to support China in commanding a significant position in the international biotechnology industry.[471]

ii. Biometric Identifiers

As previously discussed, the gathering and aggregating of biometric data can be a complex process, and much about the market for biometric data is still unknown. The legitimate use of biometrics across many areas of technology is increasing rapidly, and the exposure of biometric data to countries of concern could prove to be especially damaging since the physical characteristics linked to biometrics are often difficult or impossible to change.

The PRC already has a demonstrated ability to collect and exploit the biometric data of its citizens, an effort that has been especially targeted at oppressed groups within its population. This has included gathering data such as ''DNA samples, fingerprints, iris scans, and blood types'' and creating a database where such data is linked with an individual's personal identifier.[472] These capabilities will likely continue to be developed as the technology improves and could easily be used to undermine U.S. national security.

[457] Jan van Aken & Edward Hammond, *Genetic Engineering and Biological Weapons: New Technologies, Desires and Threats from Biological Research,* 4 EMBO Reports S57 (May 9, 2003), *https://doi.org/10.1038/sj.embor.embor860* [*https://perma.cc/Z95V-SWVL*].

[458] Off. of the Dir. of Nat'l Intel., *supra* note 91, at 25; Nat'l Counterproliferation & Biosecurity Ctr., *Biological Warfare, https://www.dni.gov/index.php/ncbc-features/1548-features-2* [*https://perma.cc/6V8M-354G*].

[459] *Huntington's Disease,* Nat'l Inst. of Health, Nat'l Inst. of Neurological Disorders & Stroke, *https://www.ninds.nih.gov/health-information/disorders/huntingtons-disease#toc-what-is-huntington-s-disease* [*https://perma.cc/YE7C-UKN2*].

[460] Nat'l Counterintel. & Sec. Ctr., *supra* note 83, at 3–4.

[461] *Id.*

[462] *Id.* at 3.

[463] *Id.*

[464] *Id.*

[465] *Id.*

[466] *Id.*

[467] *Id.*

[468] *Id.* at 4.

[469] *Id.*

[470] Needham, *supra* note 455 (''[i]n science journals and online, BGI is calling on international health researchers to send in virus data generated on its equipment, as well as patient samples that have tested positive for COVID–19, to be shared publicly via China's government-funded National GeneBank.'').

[471] *Id.*

[472] Nat'l Counterintel. & Sec. Ctr., *supra* note 83.

iii. Precise Geolocation Data

Precise geolocation data in the hands of foreign adversaries poses national security risks with respect to two areas: (1) operations, including missions, deployments, exercises, and activities of national security personnel; and (2) personnel, including those in the military and their families, as well as nonmilitary persons with the potential to obtain or hold information vital to national security.[473]

Potentially sensitive information can be gleaned outside direct conflict zones. Precise geolocation data can be readily used to identify the location and purpose of important national security-related infrastructure, facilities, and equipment, all of which could lead to immense harm to national security.

Precise geolocation data can also be used to coerce military personnel, State Department officials, and anyone else with access to sensitive national security information, including through the use of such data on their family members or other close associates.[474] Compromising information gleaned from geolocation data can be used by adversaries for surveillance and intelligence gathering as well as to extort, blackmail, dox, and manipulate behavior to obtain sensitive national security information. With all the information that is readily available from data brokers, it is quite feasible to develop effective strategies to identify national security personnel and diplomatic/foreign-policy personnel working with specific sensitive information and to track their movements and behavior.

Adversaries could use these datasets to identify where national security personnel work, then use the personnel's health or financial information to bribe or blackmail them into providing the adversaries with access to restricted systems, sensitive information, or critical programs or infrastructure. Precise geolocation data could also allow these countries to track service members' and other national security personnel's movements, impersonate personnel online or in email, and identify personnel working on specific tasks within the national security community.

Countries of concern can also exploit access to government-related data, regardless of its volume. As one report has explained, for example, location-tracking data on individuals (*e.g.,* military members, government employees and contractors, or senior government officials) can ''reveal sensitive locations—such as visits to a place of worship, a gambling venue, a health clinic, or a gay bar[,]'' or ''reputationally damaging lifestyle characteristics, such as infidelity[,]'' which ''could be used for profiling, coercion, blackmail, or other purposes[.]'' [475]

In addition, these geolocation capabilities, combined with photography, ''can expose personal information, locations, routines and numbers of [Department of Defense (DOD)] personnel, and potentially create unintended security consequences and increased risk to the joint force and mission.'' [476]

iv. Personal Health Data

Personal health data also presents threats in the hands of foreign adversaries. There are a few documented cases of data brokers selling sensitive health information to foreign governments, including those in part IV.D.1.a of this preamble. Purchasers may have direct, indirect, or undisclosed ties to foreign officials that provide these entities with access to otherwise prohibited data. The presence of foreign adversaries in the U.S. health data market makes the variety and amount of American health data available in the data-brokerage ecosystem risky. Notably, the types of sensitive personal data (*e.g.,* mental health or HIV/AIDS diagnoses) available, paired with the increasing speed and ease with which artificial intelligence and other technologies can re-identify individuals using as few as 15 demographic attributes (*e.g.,* ZIP code, date of birth, gender, citizenship, race, occupation) from another dataset, have the potential to produce harmful outcomes for the American public if placed in the wrong hands.[477]

Currently, health data brokers collect and sell a wealth of information encompassing everything from general health conditions to addiction and prescription drug use. Additional discussion of these risks associated with personal health data can be found in part V.A.4 of this preamble.

v. Personal Financial Data

Financial data tied to individuals can pose associated national security threats in the hands of foreign adversaries. There is also an associated threat to national security to U.S. persons who might be targeted for recruitment by a foreign adversary through the use of financial data as leverage over such U.S. persons. 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 and debts, and transactions; or data in a credit or ''consumer report'' expose that individual to more than monetary losses.[478] The threat of exposing an individual's spending habits, particularly spending that may be embarrassing, can render that person open to extortion or blackmail.[479] In instances where a threatened individual has access to especially sensitive information, national security may be at risk.

vi. Covered Personal Identifiers

Covered personal identifiers are a form of sensitive personal data that are both widely available and highly variable in nature. For example, covered personal identifiers may include demographic or contact data (*e.g.,* first and last name, birthplace, ZIP code, residential street or postal address, phone number, and email address and similar public account identifiers) that is linked to financial account numbers. Many types of covered personal identifiers can be used effectively in combination with other typers of sensitive personal data. The versatility of this data could make covered personal identifiers a valuable target for foreign adversaries attempting to increase the effectiveness of the bulk sensitive personal data in their possession by linking together separate datasets. For example, the PRC has both stolen data on U.S. persons that has included covered personal identifiers (*e.g.,* names and Social Security numbers, as evidenced in the 2015 hack of the health insurer Anthem, Inc.) and has effectively used personal identifiers within internal datasets on their citizens as a way to more effectively surveil marginalized groups.[480]

[473] Hazelrig, *supra* note 4; Sherman et al., *supra* note 6.

[474] Sherman et al., *supra* note 6 at 14.

[475] Sherman et al., *supra* note 6, at 15.

[476] Press Release, Def. Logistics Agency, *New Policy Prohibits DoD Employees from Using GPS Services in Operational Areas,* (Aug. 8, 2018) (quotation omitted), *https://www.dla.mil/About-DLA/News/News-Article-View/Article/1597116/new-policy-prohibits-dod-employees-from-using-gps-services-in-operational-areas/* (quoting a defense department official) [*https://perma.cc/8BNE-WU65*].

[477] Adam Tanner, *supra* note 456; Rocher et al., *supra* note 45.

[478] Ctr. for Democracy & Tech., Docket No. CFPB–2023–0020, *Response to Request for Information Regarding Data Brokers,* at 3–5 (July 15, 2023), *https://cdt.org/wp-content/uploads/2023/07/CDT-Comment-to-CFPB-on-Data-Brokers-CFPB-2023-002054.pdf* [*https://perma.cc/YTJ8-QMVW*].

[479] Arango, *supra* note 428.

[480] Nat'l Counterintel. & Sec. Ctr., *supra* note 83.

vii. Government-Related Data

It has become increasingly evident in recent years that government-related location data is at risk of being exploited by countries of concern through location information collected from electronic devices, including cell phones and fitness apps.[481] Such data can be used to not only track the movements of targeted government associates but also to link them with sensitive activities and vices, such as gambling or prostitution. This information can then be used to pressure these persons to reveal sensitive information, thereby compromising U.S. national security. Methods include malicious cyber-enabled activities, espionage, and blackmail.[482]

b. Baseline: Total Potential U.S. Population Affected by Risks

Part IV.A.1 of this preamble explains how adversaries can use their access to Americans' bulk sensitive personal data to engage in malicious cyber-enabled activities and malign foreign influence and to track and build profiles on U.S. individuals, including members of the military and government employees and contractors, for illicit purposes such as blackmail and espionage. As of July 2021, one of the largest data brokers, Acxiom, sold products that purported to cover 45.5 million current and former U.S. military personnel and 21.3 million current and former government employees.[483] The proposed rule also observes that countries of concern can exploit their access to Americans' bulk sensitive personal data to collect information on activists, academics, journalists, dissidents, political figures, and members of nongovernmental organizations or marginalized communities to intimidate them; curb political opposition; limit the freedoms of expression, peaceful assembly, or association; or enable other forms of suppression of civil liberties. Even family members of primary targets can be ensnared in such malicious activity. Finally, individuals with access to advanced intellectual property, such as semiconductor designs, could be high-value targets of countries of concern.

Tables VII–2 and VII–3 of this preamble provide estimates of the size of these targeted populations, but these figures should not be added together to calculate a single population figure, since a single individual could be a member of more than one of the communities.

Several of the estimates presented in Table VII–2 of this preamble required calculations based on certain assumptions. Because data on the number of current Federal employees provided by the Office of Personnel Management does not include employees of the U.S. Postal Service, Office of the Director of National Intelligence, or Central Intelligence Agency, data on those groups was obtained from other sources and added in separate lines. The estimated number of former Federal Government contractors was calculated by applying the economy-wide labor turnover rate from 2001 to 2023 to the number of current Federal Government contractors; the Department assumed that half of the labor turnover involved workers staying in Federal Government contracting, and half involved workers leaving the industry. The estimated number of family members of military veterans was calculated by applying the current average number of family members for current military members to the military veteran population.

TABLE VII–2—AFFECTED POPULATION—GOVERNMENT-RELATED GROUPS

Category	Population
Current Federal Government employees (excluding employees of the U.S. Postal Service, director of National Intelligence, and Central Intelligence Agency) [a]	2,271,498
U.S. Postal Service employees [b]	525,469
Office of the Director of National Intelligence employees [c]	1,750
Central Intelligence Agency employees [d]	20,000
Former Federal Government employees [e]	4,103,208
Current Federal Government contractors [f]	4,100,000
Former Federal Government contractors [f g]	1,715,850
Department of Defense active duty [h]	1,304,720
Coast Guard active duty [h]	39,485
Ready Reserve [h]	994,860
Standby Reserve [h]	5,253
Retired Reserve [h]	183,728
Current military family members [h]	2,482,499
Military veterans [i]	17,680,000
Former military family members [h i]	21,188,328

[a] U.S. Off. of Pers. Mgmt., *Status Data: Employment,* Federal Workforce Data (Feb. 2024), *https://perma.cc/7NF9-CTSC.*

[b] *Number of Postal Employees Since 1926,* U.S. Postal Service (Feb. 2024), *https://about.usps.com/who/profile/history/employees-since-1926.htm* [*https://perma.cc/6W5W-VJJ6*].

[c] Charles C. Clark, *Lifting the Lid,* Gov't Exec. (Sept. 1, 2012), *https://www.govexec.com/magazine/features/2012/09/lifting-lid/57807/* [*https://perma.cc/N8Z8-GEL8*].

[d] Michael J. O'Neal, *CIA, Formation and History,* Encylopedia.com, *https://www.encyclopedia.com/politics/encyclopedias-almanacs-transcripts-and-maps/cia-formation-and-history* [*https://perma.cc/RZ24-YJAE*].

[481] Def. Logistics Agency, supra note 476.

[482] Sherman et al., *supra* note 6 at 15.

[483] Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals* (2021), *https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf* [*https://perma.cc/Q3QL-PK7K*].

[e] U.S. Off. of Pers. Mgmt., *Dynamics Data: Separations, FY 20052005–FY 2009 (data cube),* Federal Workforce Data (Feb. 2024), *https://www.fedscope.opm.gov/ibmcognos/bi/v1/disp?b_action=powerPlayService&m_encoding=UTF-8&BZ=1AAABv9rMvcF42pVOQW6DQAz8jE2SQyOvYRM4cFjYRcmhkAYuPVXbZFNFpRAB~1cFqEraW2dkyR6PR~bKYl1WxdHsddwPbef2eonMVxOQkYFKhJbbgElZCl9xsNlkyt8mUhAyr7zx1qhjujuoahcjZ6e2GVwzIGeXtj67DmWCATX2y6GvFwd7_rQfrn8r3c12dri2Tb9AqZGz27z67XwIVPVueaMTMvsFZmYSCLTEzL9zNFqDPN0ma7Tls9NWu2LPFfPJv53kJe8xBciEEQkBAEAgSRggpEA90BkQh7TVF0jRdoO7o8EyCGyT8hOIL8jR7Mg7gJMQPZH_wPExKmbn5lqfmHGNxVvb8l%3D* [*https://perma.cc/L42Z-AFAA*]; U.S. Off. of Pers. Mgmt., *Dynamics Data, Separations, FY 2010–FY 2014* (data cube), Federal Workforce Data (Feb. 2024), *https://www.fedscope.opm.gov/ibmcognos/bi/v1/disp?b_action=powerPlayService&m_encoding=UTF-8&BZ=1AAABv4ldgp142pVOwW6CQBD9mR3UQ83sg1U4cAB2iR4KVrj01FBdG1MKBvj~NEAabW99L5PMvHnzMk6Rr4syP5q9Dvuh7exeLwm4GqmiTZAoX_vAg_~HasNbTwdBbCL4W0PAyhlvTXRMdoeo3IWE9NQ2g20GQnpp67PtSMXkcVN9WXL14lCdPqsP278V9lZ11XBtm35BShPS27z67X_wEbjsbHMm8DJ9JTBYMoGfCPwze6sxzNFFsk7yLDNJuc_zLHo24b_DnPglvDALycxSshCChWIBFiOFuAcSmDCmRXVNHOhqsH8kQfAJLhOsJLwTglmQd0FMILij~QFy4tTNz0w1vzDjG3wAb~w%3D* [*https://perma.cc/5D43-3SY8*]; U.S. Off. of Pers. Mgmt., *Dynamics Data, Separations, FY 2015–FY 2019* (data cube), Federal Workforce Data (Feb. 2024), *https://www.fedscope.opm.gov/ibmcognos/bi/v1/disp?b_action=powerPlayService&m_encoding=UTF-8&BZ=1AAABv6ePmJp42pVOQW6DQAz8jE2SQyOvFyI4cFjYReFQSAOXnqptsqmiUoiA~6sCVCXtrTOyZl~HI3tVua3q8mhyHQ9j17tcr5H5GpJvRCgCtVPCJyOjROosldpPDCU7Qci88aZbo47p~qDqfYycnbp2dO2InF265ux6DBL0qbVfDqVeHezp03644a1yN9vb8dq1wwoDjZzdltVv~4MNmeretWdkWmevyMQkAmR6QqafOdpMYZ6u0m1aFoVJ67wsCvVs4n8HeclLfCECQURCEAAQBARMMBHgHohMyFOaahqkSNvR~ZEAOUSWhOwE8jtytAjiLsAMZDnZHyBmzt3yzFzLCwu_AVRTb_0%3D* [*https://perma.cc/646G-6NBA*]; U.S. Off. of Pers. Mgmt., *Dynamics Data, Separations, FY 2020–FY 2024* (data cube), Federal Workforce Data (Feb. 2024), *https://www.fedscope.opm.gov/ibmcognos/bi/v1/disp?b_action=powerPlayService&m_encoding=UTF-8&BZ=1AAABv3dM77542pVOwW6DMAz9GZu2h1WOAa05cIAkqD0MusKlpylr06kagwr4f00BTe1223uyZD8%7EPzmoynVVlwez08kwdr3b6SUyX2PJmeFYylCrSD9HKemNyFiQkkJpEyHzKvC3Jj2o7T6ttwlyfura0bUjcn7pmrPrMc4wotZ_OQz1Ym9Pn%7EbDDW_Vu9nejteuHRYYa_T8Nq9__x9syFT3rj0j0zI%7ElpMnMj0h088crXxYoCu1VmVRGFXvyqJlX0zy76Age00uRCCISAgCAIKYgAk8Ae6B6K99Wto0SFLb0f2RAHmDHBKyE8jvyHIWxF2ACcihtz9ATJy6_Zmp5hdmfANkKW%7Ev* [*https://perma.cc/58FZ-T7VA*].

[f] David Welna & Marisa Peñaloza, *Not Expecting Back Pay, Government Contractors Collect Unemployment, Dip into Savings,* NPR (Jan. 7, 2019), *https://www.npr.org/2019/01/07/682821224/most-contractors-do-not-expect-to-get-back-pay-when-the-shutdown-ends* [*https://perma.cc/K4AW-ARFW*].

[g] U.S. Bureau of Labor Stat., *Total Separations Rate, Total Nonfarm, Not Seasonally Adjusted* (JTU000000000000000TSR), Job Openings and Labor Turnover Survey, *https://data.bls.gov/toppicks?survey=jt* [*https://perma.cc/VQQ3-7AT3*] (data extracted Sept. 2024) (select ''Total separations rate, Total nonfarm, not seasonally adjusted'' from list; then click ''Retrieve data''). Estimate is based on the average annual separations rate from 2000 to 2022. The estimate of former government officials is based on the average turnover rate for all employees in the economy.

[h] U.S. Dep't of Def., ICF, *022 Demographics: Profile of the Military Community* (2022), *https://download.militaryonesource.mil/12038/MOS/Reports/2022-demographics-report.pdf* [*https://perma.cc/TP2G-UADR*].

[i] U.S. Bureau of Labor Stat., *Population Level—Total Veterans, 18 Years and Over* (LNU00049526), Labor Force Statistics from the Current Population Survey, *https://beta.bls.gov/dataViewer/view/timeseries/LNU00049526* [*https://perma.cc/P396-7M3A*] (data extracted Feb. 2024).

The proposed rule highlights data associated with ''activists, academics, journalists, dissidents, political figures, or members of nongovernmental organizations or marginalized communities'' that could be used to ''intimidate such persons; curb political opposition; limit freedoms of expression, peaceful assembly, or association; or enable other forms of suppression of civil liberties.'' [484] Table VII–3 of this preamble describes the size of these populations.

Table VII–3 of this preamble also contains several figures that required calculations based on certain assumptions. The estimated number of activists was calculated using a survey from the *Washington Post* and Kaiser Family Foundation that asked respondents whether they considered themselves activists; the percentage that answered ''yes'' was then applied to the current adult population. No data was available on the number of people residing in the United States who would be considered dissidents, so an estimate is provided for the size of this group. For this analysis, marginalized communities were assumed to include members of the lesbian, gay, bisexual, or transgender (''LGBT'') community; religious minorities; and racial minorities.[485] The number of religious minorities was calculated using the percentage of the population that identified as Jewish, Muslim, Buddhist, Hindu, or another religion.[486]

As noted earlier in this section, the populations affected by risks have substantial overlap, so the Department is unable to provide a single estimate of the affected population. Nonetheless, these estimates show that a substantial portion of the U.S. population is currently affected by the risks resulting from adversaries' access to bulk sensitive personal data.

TABLE VII–3—POPULATIONS AFFECTED BY RISKS—OTHER GROUPS

Category	Population
Activists [a b]	46,973,153
Academics [c]	1,380,290
Journalists [d]	44,530
Dissidents [e f g h]	127,929
Political figures [i]	519,682
Members of non-governmental organizations [j]	715,790
Marginalized communities—LGBT [k]	13,942,200
Marginalized communities—Religious [b l]	14,352,908

[484] 89 FR 15781.

[485] The groups that were assumed to be marginalized communities are similar to the groups most likely to be targeted in one or more countries of concern, which differs from the definition of underserved communities defined in Executive Order 13985 (Advancing Racial Equity and Support for Underserved Communities Through the Federal Government), 89 FR 7009 (Jan. 20, 2021). For examples of LGBT, religious, and racial minorities being targeted in the countries of concern, *see, e.g.,* Bibek Bhandari & Elgar Hu, *'Rainbow Hunters' Target LGBTQ Chinese Students,* Foreign Policy (July 28, 2023), *https://foreignpolicy.com/2023/07/28/china-rainbow-hunters-target-lgbtq-students/* [*https://perma.cc/UZ37-D48A*]; Pew Rsch. Ctr., *Government Policy Toward Religion in the People's Republic of China—A Brief History,* Measuring Religion in China (Aug. 30, 2023), *https://www.pewresearch.org/religion/2023/08/30/government-policy-toward-religion-in-the-peoples-republic-of-china-a-brief-history/* [*https://perma.cc/25CH-7AKH*].

[486] People who identify as Jewish, Muslim, Buddhist, Hindu, or members of other religions are non-Christian populations that each represent less than 2 percent of the U.S. population. *2022 PRRI Census of American Religion: Religious Affiliation Updates and Trends,* PRRI (Feb. 24, 2023), *https://www.prri.org/spotlight/prri-2022-american-values-atlas-religious-affiliation-updates-and-trends/* [*https://perma.cc/BQA7-MK2J*].

TABLE VII–3—POPULATIONS AFFECTED BY RISKS—OTHER GROUPS—Continued

Category	Population
Marginalized communities—Race[m] (white Hispanic population not included)	130,398,545

[a] Wash. Post & Kaiser Family Found., *Survey on Political Rallygoing and Activism* (Apr. 2018), *https://files.kff.org/attachment/Topline-Washington-Post-Kaiser-Family-Foundation-Survey-on-Political-Rallygoing-and-Activism* [*https://perma.cc/7ELT-NM6L*].
[b] U.S. Census Bureau, *K200104: Population by Age,* American Community Survey, 1-Year Supplemental Estimates (2022), *https://data.census.gov/table/ACSSE2022.K200104* [*https://perma.cc/D6KP-JTKD*].
[c] U.S. Bureau of Labor Stat., *25–1000: Postsecondary Teachers,* National Occupational Employment and Wage Estimates (May 2023), *https://www.bls.gov/oes/current/oes_nat.htm* [*https://perma.cc/8FTZ-FCMW*].
[d] U.S. Bureau of Labor Stat., *27–3023: News Analysts, Reporters and Journalists,* National Occupational Employment and Wage Estimates (May 2023), *https://www.bls.gov/oes/current/oes_nat.htm* [*https://perma.cc/8FTZ-FCMW*].
[e] U.S. Dep't of Homeland Sec., Off. of Immigr. Stat., *2003 Yearbook of Immigration Statistics* (2004), *https://www.dhs.gov/ohss/topics/immigration/yearbook/2003* [*https://perma.cc/FSJ3-XRSG*].
[f] U.S. Dep't of Homeland Sec., Off. of Immigr. Stat., *2012 Yearbook of Immigration Statistics* (2013), *https://www.dhs.gov/ohss/topics/immigration/yearbook/2012* [*https://perma.cc/XZG6-WL65*].
[g] U.S. Dep't of Homeland Sec., Off. of Immigr. Stat., *2022 Yearbook of Immigration Statistics* (2023), *https://www.dhs.gov/ohss/topics/immigration/yearbook/2022* [*https://perma.cc/9YXU-Y2EF*].
[h] U.S. Dep't of Just., Exec. Off. for Immigr. Rev., *Adjudication Statistics: Asylum Decision Rates by Nationality* (2023), *https://www.justice.gov/eoir/page/file/1107366/dl* [*https://perma.cc/PJ7C-GRK4*].
[i] *How Many Politicians Are There in the USA?* PoliEngine, *https://poliengine.com/blog/how-many-politicians-are-there-in-the-us* [*https://perma.cc/D5DG-KJHM*].
[j] Ctr. on Nonprofits, Philanthropy, and Soc. Enter., George Mason U., *Nonprofit Employment Data Project Jobs Recovery Data Dashboard* (Jan. 10, 2023), *https://nonprofitcenter.schar.gmu.edu/nonprofit-employment-data-project/resources-and-dashboards/* [*https://perma.cc/2XBZ-ACDW*].
[k] Andrew R. Flores & Kerith J. Conron, *Adult LGBT Population in the United States,* Williams Inst., UCLA Sch. of L. (2023), *https://williamsinstitute.law.ucla.edu/publications/adult-lgbt-pop-us/* [*https://perma.cc/MZQ2-EAP9*].
[l] *2022 PRRI Census of American Religion: Religious Affiliation Updates and Trends,* PRRI (Feb. 24, 2023), *https://www.prri.org/spotlight/prri-2022-american-values-atlas-religious-affiliation-updates-and-trends/* [*https://perma.cc/BQA7-MK2J*].
[m] U.S. Census Bureau, *K200201: Race,* American Community Survey, 1-Year Supplemental Estimates (2022), *https://data.census.gov/table/ACSSE2022.K200201* [*https://perma.cc/XJ3V-LH8J*].

c. Summary of Baseline (Without the Proposed Rule)

As stated in part IV.A.1 of this preamble, the government-related data or bulk U.S. sensitive personal data discussed here may, under certain conditions, be used against individuals—such as members of the military, government employees, and government contractors—for illicit purposes, including blackmail and espionage. The risks of any particular individual or group being targeted may vary depending on the circumstances, and these data illustrate the range of such activities. Countries of concern can also use access to government-related data or Americans' bulk U.S. sensitive personal data to collect information on activists, academics, journalists, dissidents, political figures, and members of nongovernmental organizations or marginalized communities to intimidate such persons; curb political opposition; limit freedoms of expression, peaceful assembly, or association; or enable other forms of suppression of civil liberties.

The individuals within the subgroups most at risk of having their sensitive personal data exploited by countries of concern not only play important roles in American society, but also make up a large portion of the population. When we consider that threats to the spouses and children of targeted individuals could also be made, the Department estimates that the total population of individuals who could potentially be targeted is well over 100 million individuals. Thus, the total number of those who are at risk of being targeted by foreign adversaries could exceed one-third of the entire American population. Failing to prevent the current and future sale or transfer of government-related data or bulk U.S. sensitive personal data to countries of concern effectively forgoes all the benefits that may be realized from such an action. Given the nature of the benefits to be gained from protecting national security and foreign policy from malicious actors, these benefits are unable to be monetized or quantified but will be contrasted with the estimated costs of the proposed regulation.

6. Alternative Approaches

In addition to the proposed action, the Department considered two alternatives. The first alternative, the No Action alternative, would take no regulatory action and allow the unrestricted transfer of bulk U.S. sensitive personal data to any foreign company, person, or country, including the countries of concern. The No Action alternative would not achieve the benefits of reducing the risks to the targeted populations or to U.S. national security and foreign policy. The growing threats related to foreign adversaries' use of bulk U.S. sensitive personal data, enhanced by advancing technologies such as artificial intelligence, for purposes of subjecting American citizens to exposure to blackmail and other malicious actions would continue. In addition to the sale of bulk U.S. sensitive personal data, the vendor, employment, and investment agreements would also continue without restrictions, as would the risks that the proposed rule is intended to reduce. Of course, the No Action alternative would also result in no additional costs to industry. As explained in part VII.A.7 of this preamble, however, the Department considers the expected benefits of the proposed regulation to greatly exceed the estimated costs, resulting in net benefits that are not realized by the No Action alternative. Therefore, the Department rejects the No Action alternative.

The second alternative considered was a prohibition of the transfer to countries of concern of all data that would fall within the scope of the proposed rule. This alternative would go further than directed by the Order, the provisions of which were directed at bulk U.S. sensitive personal data and would entail more complicated and costly enforcement efforts than the proposed rule. Since this alternative would prohibit not only bulk U.S. sensitive personal data but also small transfers of sensitive personal data that may not present any marginal substantial risk to national defense or foreign policy, the small additional benefits are not likely to justify the much larger value of lost transactions and compliance costs than the proposed rule's estimated cost of $502 million.

Since the marginal costs of this alternative over the costs of the proposed regulation are expected to be larger than the marginal benefits—if there are any—associated with it, this alternative would necessarily have lower net benefits, as measured by total benefits less total costs.

More generally, in addressing proposals from commenters, the Department also considered alternatives that could broaden the scope of the rule (and thus potentially be more costly) or narrow its scope (and thus potentially be less costly). These alternatives include, for example, lowering or increasing the proposed bulk thresholds, prohibiting or restricting (instead of exempting) additional categories of transactions such as those involving telecommunications or clinical-trial data, expanding the list of countries of concern, and expanding the categories of covered persons. The Department declined to adopt them because they would appear not to appropriately tailor the proposed rule to the national security risks and could cause unintended economic effects, for the reasons more fully discussed with respect to those proposals.

7. Benefits of the Proposed Rule

As mentioned in part VII.A.2 of this preamble, the benefits of the proposed rule associated with reducing threats to national security and foreign policy are difficult to measure. While these benefits are difficult to measure, there is a liberal opportunity for foreign adversaries to access and exploit Americans' sensitive data without the proposed rule. This situation and the best-available information indicate that there is a high likelihood of harm to national security and that the harm to national security could be high, suggesting that the expected benefits of the proposed rule exceed its expected costs. Alternatively, even if the likelihood of harm to national security is low in some circumstances, the potential damage to national security remains high, suggesting that even modest risk reductions are justified.

The proposed rule focuses on the risk of access to government-related data or bulk U.S. sensitive personal data by countries of concern and covered persons. Countries of concern can use their access to Americans' bulk sensitive personal data to engage in malicious cyber-enabled activities and malign foreign influence as well as to track and build profiles of U.S. individuals, including members of the military and Federal employees and contractors, for illicit purposes such as blackmail and espionage. Countries of concern can also exploit their access to Americans' bulk sensitive personal data to collect information on activists, academics, journalists, dissidents, political figures, and members of nongovernmental organizations or marginalized communities to intimidate them; curb political opposition; limit freedoms of expression, peaceful assembly, or association; or enable other forms of suppression of civil liberties. Nongovernmental experts have underscored these risks.

Reducing these threats may produce many qualitative benefits, such as improving the security of the American people and safeguarding democratic values, all of which are beyond a reasonable, reliable, and acceptable estimate of quantified monetary value. Other benefits may also arise, such as the creation of new businesses to provide vetting information to firms seeking entrance into the restricted transactions market, or advancements in overall industry cybersecurity technology that result in more secure systems. We make no attempt to quantify these potential benefits, but we welcome comments that may allow us to do so.

8. Costs of the Proposed Rule

The economic costs of the proposed rule are the lost economic value of the covered transactions that are prohibited or forgone, referred to as ''direct costs,'' and the costs of compliance (for restricted transactions, the cost of complying with the security requirements established by DHS/CISA, affirmative due diligence requirements, audit requirements, and affirmative reporting requirements).

Other provisions included in the regulations—including regulations of investment, employment, and vendor agreements through the imposition of security requirements—will have a mixture of economic impacts, such as one-time costs of switching to approaches that will comply with new regulations, and economic benefits, such as improved cybersecurity controls.

The challenge of estimating the economic impact with any degree of precision is that, because there are no regulations prohibiting cross-border bulk U.S. sensitive personal data transactions, currently available data provides incomplete, unreliable, or irrelevant estimates of the types, volume, and value of the bulk U.S. sensitive personal data transfer activity and thus creates uncertainty in estimates of lost value due to the proposed rule.

Similarly, the estimates of the costs of requirements for affirmative due diligence, security, recordkeeping, affirmative reporting, and audits are very preliminary in this analysis because the size of the industry, per-company costs, and per-transaction costs are very difficult to estimate precisely. Furthermore, based on its experience with similar regulations related to economic sanctions and export controls, the Department expects the costs of compliance with this proposed rule to vary significantly across companies.

Our estimates reflect costs for firms that currently engage in transactions involving bulk U.S. sensitive personal data. The universe of firms that engage in transactions involving bulk U.S. sensitive personal data is larger than the subset of such firms that knowingly transfer such data to countries of concern or covered persons; this larger universe of firms will need to undertake some due diligence measures to ensure that their typical data transfers are not in fact going to countries of concern or covered persons. Comments are solicited and welcome on the estimates that follow.

a. Value of Lost and Forgone Transactions

The costs of the proposed rule would include the economic value of lost or forgone transactions related to the sale, transfer, and licensing of bulk U.S. sensitive personal data, as well as biospecimens, to the six countries of concern. These lost or forgone transactions would include transactions that are prohibited as well as covered data transactions that are forgone because an entity decides not to bear the costs of complying with the due diligence and security requirements necessary to engage in a restricted transaction.

The total economic value of lost and forgone transactions should not exceed the total economic value of such exports to these countries of concern, as, all else equal, an entity would forgo a transaction if its expected compliance costs exceed the expected economic value of the transaction. The anticipated value of potentially regulated transactions with all countries of concern except China is negligible, given the lack of general cross-border transactions involving bulk sensitive personal data and the existing impediments to trade, such as economic sanctions. More specifically, in recent years, the proportions of U.S. bidirectional trade and investment

represented by trade with Iran,[487] North Korea,[488] and Cuba,[489] respectively, have been negligible or unknown. Trade with Venezuela represents 0.1 percent of U.S. totals.[490]

Trade with Russia averaged about 0.5 percent of all U.S. trade from 2014 to 2023, dropping to 0.1 percent in 2023.[491] U.S. cross-investment (*i.e.,* two-way foreign direct investment) [492] with Russia averaged about 0.2 percent of total U.S. foreign cross-investment from 2013 to 2022.[493] In contrast, the respective shares of U.S. imports/exports and cross-investment that are conducted with China have averaged about 12 percent and 1.3 percent, respectively, during the same periods.[494] Given this, the estimation of the economic costs of lost or forgone transactions here focuses primarily on China, although Russia is also considered.

Similarly, foreign direct investment into the United States from countries of concern in the information industry is a relatively small portion of the total level of foreign direct investment in this sector. Chinese investment, which has been the highest among countries of concern, has been steadily falling over the past several years. Foreign direct investment figures, based on the country of the ultimate beneficial owner and the country of direct foreign ownership, are presented in Tables VII–4 and VII–5 of this preamble.

TABLE VII–4—FOREIGN DIRECT INVESTMENT POSITION IN THE UNITED STATES ON A HISTORICAL-COST BASIS IN THE INFORMATION INDUSTRY BY COUNTRY OF ULTIMATE BENEFICIAL OWNER

[millions of dollars]

	2016	2017	2018	2019	2020	2021	2022
All Countries Total	171,474	197,266	208,932	204,950	182,913	259,867	254,691
China	1,806	2,413	2,286	2,936	1,700	1,432	452
Hong Kong	366	416	148	562	413	429	417
Venezuela	(*)	(*)	−3	−5	−6	−7	(D)
China + Hong Kong Share	1.3%	1.4%	1.2%	1.7%	1.2%	0.7%	0.3%
Venezuela Share	n/a	n/a	0.0%	0.0%	0.0%	0.0%	n/a

Note: (*) indicates a nonzero value that rounds to zero. (D) indicates that the data in the cell have been suppressed to avoid disclosure of data of individual companies.

Source: U.S. Bureau of Econ. Analysis, *Balance of Payments and Direct Investment Position Data: Foreign Direct Investment in the U.S., Foreign Direct Investment Position in the United States on a Historical-Cost Basis, Country of UBO and Industry (NAICS) (Millions of Dollars), https://apps.bea.gov/iTable/?ReqID=2&step=1&_gl=1*ubcfnx*_ga*MjEzMzE0NDY0Ny4xNzA1NTc5Mjcw*_ga_J4698JNNFT*MTcyMDYzNjY0My44Mi4xLjE3MjA2MzgzMzQuNTMuMC4w#eyJhcHBpZCI6Miwic3RlcHMiOlsxLDIsMyw0LDUsNywxMF0sImRhdGEiOltbIlN0ZXAxUHJvbXB0MSIsIjIiXSxbIlN0ZXAxUHJvbXB0MiIsIjEiXSxbIlN0ZXAyUHJvbXB0MyIsIjEiXSxbIlN0ZXAzUHJvbXB0NCIsIjIyII0sWyJTdGVwNFByb21wdDUiLCIyMiJdLFsiU3RlcDVQcm9tcHQiwiMSJdLFsiU3RlcDdQcm9tcHQ4IixbIjI4LDI5LDMwLDMxLDMyLDMzLDM0LDM1LDM2LDM3LDM4LDM5LDQwLDQxLDQyLDQzLDQ4LDQ5LDUyLDU1LDU2LDU4LDY1LDY2Il1dLFsiU3RlcDhQcm9tcHQ5QSIsWyI3Il1dLFsiU3RlcDhQcm9tcHQxMEEiLFsiMSJdXV19* [*https://perma.cc/X7SK-2LD8*].

TABLE VII–5—FOREIGN DIRECT INVESTMENT POSITION IN THE UNITED STATES ON A HISTORICAL-COST BASIS IN THE INFORMATION INDUSTRY BY COUNTRY OF DIRECT FOREIGN PARENT

[millions of dollars]

	2016	2017	2018	2019	2020	2021	2022
All Countries Total	171,474	197,266	208,932	204,950	182,913	259,867	254,691
China	134	(D)	4,286	4,882	3,480	2,809	772
Hong Kong	(D)	(D)	−53	389	284	282	196
Venezuela	−4	(D)	−3	−2	−2	(*)	(D)
China + Hong Kong Share	n/a	n/a	2.0%	2.6%	2.1%	1.2%	0.5%
Venezuela Share	0.0%	n/a	0.0%	0.0%	0.0%	N/A	N/A

Note: (*) indicates a nonzero value that rounds to zero. (D) indicates that the data in the cell have been suppressed to avoid disclosure of data of individual companies.

Source: U.S. Bureau of Econ. Analysis, *Balance of Payments and Direct Investment Position Data: Foreign Direct Investment in the U.S., Foreign Direct Investment Position in the United States on a Historical-Cost Basis, By Country and Industry (NAICS) (Millions of Dollars) https://apps.bea.gov/iTable/?ReqID=2&step=1&_gl=1*ay559c*_ga*MTM5ODMzNTkyNy4xNzEwMjgzOTY0*_ga_J4698JNNFT*MTcyMjk0ODk5My4yNi4xLjE3MjI5NTA2NTEuNTcuMC4w#eyJhcHBpZCI6Miwic3RlcHMiOlsxLDIsMyw0LDUsNywxMF0sImRhdGEiOltbIlN0ZXAxUHJvbXB0MSIsIjIiXSxbIlN0ZXAxUHJvbXB0MiIsIjEiXSxbIlN0ZXAyUHJvbXB0MyIsIjEiXSxbIlN0ZXAzUHJvbXB0NCIsIjIyII0sWyJTdGVwNFByb21wdDUiLCIyMiJdLFsiU3RlcDVQcm9tcHQiwiMSJdLFsiU3RlcDdQcm9tcHQ4IixbIjI4LDI5LDMwLDMxLDMyLDMzLDM0LDM1LDM2LDM3LDM4LDM5LDQwLDQxLDQyLDQzLDQ4LDQ5LDUyLDU1LDU2LDU4LDY1LDY2Il1dLFsiU3RlcDhQcm9tcHQ5QSIsWyI3Il1dLFsiU3RlcDhQcm9tcHQxMEEiLFsiMSJdXV19=* [*https://perma.cc/NH7V-GZNU*].

[487] U.S. Census Bureau, *Trade in Goods with Iran, https://www.census.gov/foreign-trade/balance/c5070.html* [*https://perma.cc/EAZ7-PJU2*].

[488] U.S. Census Bureau, *Trade in Goods with Korea, North, https://www.census.gov/foreign-trade/balance/c5790.html* [*https://perma.cc/NY7X-DRBA*].

[489] U.S. Census Bureau, *Trade in Goods with Cuba, https://www.census.gov/foreign-trade/balance/c2390.html* [*https://perma.cc/CUF2-FWWY*].

[490] U.S. Bureau of Econ. Analysis, *U.S. International Trade in Goods and Services, Venezuela,* Venezuela—International Trade and Investment Country Facts, *https://apps.bea.gov/international/factsheet/factsheet.html#219* [*https://perma.cc/2K9N-YGFS*].

[491] U.S. Bureau of Econ. Analysis, *U.S. International Trade in Goods and Services, Russia,* Russia—International Trade and Investment Country Facts, *https://apps.bea.gov/international/factsheet/factsheet.html#341* [*https://perma.cc/GF8U-6GK2*].

[492] Mark Casson & Nigel Wadeson, *Cross-Investments by Multinationals: A New Perspective,* 14 Glob. Strategy J. 279, 279–80 (2023) (defining cross-investment as ''where firms conduct FDI into each other's home countries'').

[493] U.S. Bureau of Econ. Analysis, *supra* note 491.

[494] *U.S. International Trade in Goods and Services, China,* China—International Trade and Investment Country Facts, *https://apps.bea.gov/international/factsheet/factsheet.html#650* [*https://perma.cc/X7QF-CYXH*].

Note that some fraction of the lost or forgone data transactions may be for beneficial uses. Beneficial uses of bulk U.S. sensitive personal data in the countries of concern may include consumer-choice improvements and the use of artificial intelligence to expedite innovation in drug discovery and increase knowledge of patterns of, for example, consumption, commerce, transportation, traffic, information/news transmission, nutrition, and health.

The following analysis relies in part on data available from the BEA on U.S. exports of telecommunications, computer, and information services, both in total and for each of the three sub-categories, to China and Russia. Tables VII–6 and VII–7 of this preamble rely on an analysis of the BEA data to approximate the value of lost transactions.

i. Global Market Value of Genomic, Biometric, and Location Data

Genomic data includes data that is used in drug discovery and development, specifically in developing products such as systems, software, and reagents, and in developing processes such as cell isolation, sample preparation, and genomic analysis.[495] Biometric data is used in consumer electronics and automotive applications for safety, surveillance, and identification methods, including facial, posture, voice, fingerprint, and iris recognition technologies.[496] Location data is used in smart devices, network services for improved connectivity, systems integration, monitoring, and satellite location technology, as well as to produce timely, relevant and personalized offers/information for customers.[497]

According to market research data from one company,[498] the global genomics market's value is estimated at $27.58 billion in 2021, $32.56 billion in 2022, and, given an estimated compound annual growth rate of 18.2 percent, $38.49 billion in 2023 and $45.49 billion in 2024.[499] One estimate of the global biometric technology market values it at $34.27 billion in 2022 and, given an estimated 20.4 percent compound annual growth rate, $41.26 billion in 2023 and $49.68 billion in 2024.[500] Finally, one estimate values the global location data market at $18.52 billion in 2023 and, given an estimated 15.6 percent compound annual growth rate, $21.41 billion in 2024.[501] Table VII–6 of this preamble presents these global totals for genomic, biometric, and location data estimates.[502]

TABLE VII–6—GLOBAL TECHNOLOGY MARKET VALUE ESTIMATES FOR GENOMIC, BIOMETRIC, AND LOCATION DATA FOR 2021–2024 (IN BILLIONS OF 2022 DOLLARS) WITH COMPOUND ANNUAL GROWTH RATE (''CAGR'')

Data type	2021	2022	2023	2024	CAGR (%)
Genomic [a]	$27.58	$32.56	$38.49	$45.49	18.2
Biometric [b]	.....	34.27	41.26	49.68	20.4
Location [c]	.....	.....	18.52	21.41	15.6

[a] *Genomics Global Market to Reach $63.5 Billion in 2026 at a CAGR of 18.2%,* Globe Newswire (Sept. 6, 2022), *https://www.globenewswire.com/en/news-release/2022/09/06/2510235/28124/en/Genomics-Global-Market-to-Reach-63-5-Billion-in-2026-at-a-CAGR-of-18-2.html* [*https://perma.cc/SUV8-VVMK*].

[b] Grand View Research, Report ID No. 978–1–68038–299–0, *Biometric Technology Market Size, Share & Trends Analysis Report, 2023–2030* (2023), *https://www.grandviewresearch.com/industry-analysis/biometrics-industry* [*https://perma.cc/KN36-3KZW*].

[c] Grand View Research, Report ID No. GVR–2–68038–401–7, *Location Intelligence Market Size, Share & Trends Analysis Report, 2024–2030* (2024), *https://www.grandviewresearch.com/industry-analysis/location-intelligence-market* [*https://perma.cc/WS6U-2324*].

ii. U.S. Exports to Relevant Specific Categories and to Countries of Concern

Data is available on U.S. exports in the category of telecommunications, computer, and information services, both in total and for each of these three service subcategories, to China and Russia.[503] Data on exports in a relevant sub-category of information services—database and other information services—is available globally and for both China and Russia individually.

Telecommunications, Computer, and Information Services is one of the eleven service categories BEA presents in the U.S. international transactions accounts. The Telecommunications Services sub-category includes basic services (*e.g.,* transmitting messages between destinations) as well as value-added and support services. The Computer Services sub-category includes software, computing and data-storage services, hardware and software consultancy, and licensing agreements tied to downloading applications. The category of information services includes database services and web search portals, which belong to one subcategory, and news agency services, which belong to the other.[504] This Database Services sub-category includes data brokers.

Table VII–7 of this preamble presents the value of U.S. exports of telecommunications services, computer services, information services, and the database and other information services component of information services. The table also reports exports to China for the three components combined and the exports to China and Russia individually for database and other information services.

[495] *Genomics Global Market to Reach $63.5 Billion in 2026 at a CAGR of 18.2%,* Globe Newswire (Sept. 6, 2022), *https://www.globenewswire.com/en/news-release/2022/09/06/2510235/28124/en/Genomics-Global-Market-to-Reach-63-5-Billion-in-2026-at-a-CAGR-of-18-2.html* [*https://perma.cc/SUV8-VVMK*].

[496] Grand View Research, Report ID No. 978–1–68038–299–0, *Biometric Technology Market Size, Share & Trends Analysis Report, 2023–2030* (2023), *https://www.grandviewresearch.com/industry-analysis/biometrics-industry* [*https://perma.cc/KN36-3KZW*].

[497] Grand View Research, Report ID No. GVR–2–68038–401–7, *Location Intelligence Market Size, Share & Trends Analysis Report, 2024–2030* (2024), *https://www.grandviewresearch.com/industry-analysis/location-intelligence-market* [*https://perma.cc/WS6U-2324*].

[498] *Genomics Global Market to Reach $63.5 Billion in 2026 at a CAGR of 18.2%, supra* note 495.

[499] *Id.*

[500] Grand View Research, *supra* note 496.

[501] Grand View Research, *supra* note 497.

[502] The Department notes several caveats with the Grand View Research estimates shown in Tables VII–4 and VII–5 of this preamble, including non-transparent methods for gathering data and producing estimates, a non-statistical sample of firms that may not be statistically representative of the industry, and non-response bias from interviewees from the firms.

[503] U.S. Bureau of Econ. Analysis, *U.S. International Economic Accounts: Concepts and Methods,* at 248 (June 2023), *https://www.bea.gov/system/files/2023-06/iea-concepts-methods-2023.pdf* [*https://perma.cc/8M48-Q2ZG*].

[504] *Id.*

TABLE VII–7—U.S. EXPORTS OF TELECOMMUNICATIONS, COMPUTER, AND INFORMATION SERVICES

[In billions of 2023 dollars]

Service	All	China	Russia
Components			
Telecommunications Services	$9.329	$0.095	$0.041
Computer Services	$50.328	$1.847	$0.113
Information Services	$10.972	$0.318	$0.034
Total Value	$70.629	$2.260	$0.188
Percentage of Total	100%	3.20%	0.27%
Database and Other Information Services			
Value	$10.768	*$0.318	$0.032
Percentage of Total	100%	2.94%	0.30%

Source: U.S. Bureau of Econ. Analysis, *International Transactions, International Services, and International Investment Position Tables,* Tables 2.2, *https://www.bea.gov/itable/direct-investment-multinational-enterprises* [*https://perma.cc/9XWQ-A8YQ*] (last updated July 23, 2024).

*An upper bound for 2023 is $0.318.

The $10.768 billion Database and Other Information Services sub-category comprises most (98.1 percent) of the $10.972 billion Information Services category, with the other $0.275 billion (2.6 percent) in the News-Agency Services category. For the Database and Other Information Services sub-category, U.S. exports to China are $0.318 billion ($318 million) for 2023, which is 2.94 percent of the U.S. export total. U.S. exports to Russia are $0.32 billion ($32 million), which is 0.30 percent of the U.S. export total.

These U.S. export estimates are significantly over-inclusive, as they include many kinds of data that are explicitly excluded from regulation under the proposed rule, such as web browser history and other expressive data, in addition to services that do not involve data transfer at all. Consequently, the estimates of the costs due to lost or foregone transactions resulting from the proposed rule are probably overstated.

Tables VII–6 and VII–7 of this preamble comprise the ''raw'' data on U.S. exports to countries of concern that provide upper-bound estimates of the value of lost or forgone transactions. Given the available data that informs the following analysis, the Department welcomes comments on the use of this data and on any alternative or additional data that could also be employed.

iii. Estimates of U.S. Exports of Genomic, Biometric, and Location Data

This section provides estimates of U.S. revenue from sales for three categories of data covered under the proposed rule for which data on the global market are available: genomic, biometric, and location data.

Given the lack of available published estimates of the value of U.S. exports of such data to China, Russia, and other countries of concern, the Department developed a multi-step method for estimating the value of lost transactions in genomic, biometric, and location data to the countries of concern. To summarize, we began with market research companies' estimates of the size of the global markets in geometric, biometric, and location data shown in Table VII–6 of this preamble. Then we derived estimates of the value of lost transactions through a three-step process that involved estimating the U.S. share (domestic plus export) of the global market, estimating the percentage of U.S. global sales that are domestic, and finally making some data-informed assumptions about the share of global sales in those industries that were to the countries of concern.

In 2022, the total value of the U.S. location data market was $4.20 billion, with a projected compound annual growth rate of 13.6 percent.[505] Based on these estimates, it can be projected that the U.S. portion in 2023 would be $4.77 billion ($4.20 * 1.136 = $4.77). As shown in Table VII–6 of this preamble, the market research company estimated that the global market value of location data in 2023 was $18.52 billion, so the estimated U.S. portion in 2023 would constitute 25.76 percent of that estimated global value ($4.77/$18.52 = 0.2576). Because the market research company estimated the U.S. compound annual growth rate for location data to be 13.6 percent and the global compound annual growth rate to be 15.6 percent, it can be projected that the U.S. portion of the global market in 2024 would fall slightly, from 25.76 percent to 25.31 percent (($4.77 * 1.136)/($18.52 * 1.156) = 0.2531).

The market research company estimated that the North American revenue share of the global biometric technology market in 2022 was 30.7 percent.[506] If Canada and Mexico were responsible for 5 percent of global market value, then the U.S. share of the global biometric data market in 2022 would be 25.7 percent, nearly the same as the portion for location data in 2023. Given the alignment in our estimates of the U.S. market share for location and biometric data markets, we assume that the estimated U.S. location data market in 2024 (25.31 percent) also applies to the U.S. portion of global genomic and biometric data. With that assumption, we estimate that the U.S. genomic data market is worth $12.57 billion in 2024 (25.31 percent of $49.68 billion (from Table VII–6 of this preamble)), and the U.S. market is worth $5.42 billion (25.31 percent of $21.41 billion). Table VII–8 of this preamble provides 2024 estimates of U.S. revenue (foreign plus domestic) for those three industries.

Next, the Department assumes that U.S. exports in genomic, biometric, and location data constitute 30 percent of total U.S. revenue (domestic sales plus exports). This assumption is based on market research from a U.S.-based company,[507] which estimated that in

[505] Grand View Research, *supra* note 497.

[506] Grand View Research, *supra* note 496.

[507] Market research data includes: *Genomics Global Market to Reach $63.5 Billion in 2026 at a CAGR of 18.2%, supra* note 495; Grand View Research, *supra* note 496; Grand View Research, *supra* note 497.

2017, 30 percent of revenue for data brokerage companies came from international sales. When applying this assumption to revenue from sales of genomic, biometric, and location data, we estimate that exports of U.S. genomic data in 2023 were worth $3.454 billion for genomic data (30 percent of $11.513 billion); exports of biometric data were worth $3.772 billion (30 percent of $12.574 billion); and exports of location data were worth $1.626 billion (30 percent of $5.419 billion). Table VII–8 of this preamble presents estimated revenue from U.S. exports (Step 2) alongside the other estimates from which it was derived.

TABLE VII–8—ESTIMATED REVENUE FROM INTERNATIONAL SALES OF GENOMIC, BIOMETRIC, AND LOCATION DATA IN 2023

[In billions of 2024 dollars]

Category of data	Global revenue (from Table VII-6) [a]	U.S. revenue (domestic sales + exports) [b]	Revenue from U.S. exports [c]
Genomic	$45.49	$11.51	$3.45
Biometric	$49.68	$12.57	$3.77
Location	$21.41	$5.42	$1.63
Total	$116.58	$29.51	$8.85
U.S. Revenue Share of Global Total	.....	25.31%	.....
U.S. Export Share of U.S. Revenue	.....	.....	30%

[a] *Genomics Global Market to Reach $63.5 Billion in 2026 at a CAGR of 18.2%,* Globe Newswire (Sept. 6, 2022), *https://www.globenewswire.com/en/news-release/2022/09/06/2510235/28124/en/Genomics-Global-Market-to-Reach-63-5-Billion-in-2026-at-a-CAGR-of-18-2.html* [*https://perma.cc/SUV8-VVMK*]; Grand View Research, Report ID No. 978–1–68038–299–0, *Biometric Technology Market Size, Share & Trends Analysis Report, 2023–2030* (2023), *https://www.grandviewresearch.com/industry-analysis/biometrics-industry* [*https://perma.cc/KN36-3KZW*]; Grand View Research, Report ID No. GVR–2–68038–401–7, *Location Intelligence Market Size, Share & Trends Analysis Report, 2024–2030* (2024), *https://www.grandviewresearch.com/industry-analysis/location-intelligence-market* [*https://perma.cc/WS6U-2324*].

[b] Department of Justice estimates based on global revenue data from Table VII–6 of this preamble. U.S. Revenue (Domestic Sales + Exports) is assumed to be 25.31 percent of the total global revenue for each category of data.

[c] Department of Justice estimates based on data in global revenue data from Table VII–6 of this preamble. Revenue from U.S. exports is assumed to be 30 percent of the U.S. revenue for each category of data.

To reiterate, the Department assumes that U.S. exports in genomic, biometric, and location data constitute 30 percent of total U.S. revenue (domestic sales plus exports). The Department uses this assumption to inform the analysis throughout part VII of this preamble.

iv. Estimates of U.S. Exports of Genomic, Biometric, and Location Data to the Six Countries of Concern

As delineated above in this section, the current value of potentially regulated transactions with all countries of concern except China and, to a lesser degree, Russia is negligible, given the lack of general cross-border trade in data and data-driven services and the general impediments to trade with these countries of concern, such as economic sanctions. We therefore focus this part of the analysis on China, and to a lesser degree on Russia due to the $32 million in U.S. exports of database and other information services to Russia.[508] The Department lacks data on cross-border transfers of genomic, biometric, and location data other than sales. An example of such cross-border transfers may include transfer of data within multinational companies.

As set forth in Table VII–7 of this preamble and the subsequent discussion in part VII.A.8.a.ii of this preamble, 3 percent (0.032 = $0.318 of $10.768 billion) of U.S. exports of database and other information services are currently to China and 1 percent are to Russia (0.0106 = $0.111 of $10.768 billion). Applying these percentages to the value of U.S. exports of genomic, biometric, and location data set forth in Table VII–8 of this preamble yields estimates for the value of U.S. exports of genomic, biometric, and location data to China and Russia. The estimates for U.S. exports of genomic, biometric and location data to China total $267 million and to Russia total $94 million.

TABLE VII–9—ESTIMATES OF U.S. EXPORTS OF GENOMIC, BIOMETRIC, AND LOCATION DATA TO CHINA AND RUSSIA

[In billions of 2022 dollars]

Category of data	U.S. exports (from table VII–8)	U.S. exports to China [a]	U.S. exports to Russia [b]
Genomic	$3.45	$0.10	$0.04
Biometric	$3.77	$0.11	$0.04
Location	$1.63	$0.05	$0.02
Total	$8.85	$0.27	$0.10
China share of U.S. exports	.....	3.02%	.....
Russia share of U.S. exports	.....	.....	1.06%

[a] Revenue from U.S. exports to China is assumed to be 3.02 percent of total revenue from U.S. exports for each category of data.

[b] Revenue from U.S. exports to Russia is assumed to be 1.06 percent of total revenue from U.S. exports for each category of data.

[508] *See* discussion in part VII.A.8.a of this preamble.

Source: Department of Justice estimates based on market research data from U.S.-based company, including: *Genomics Global Market to Reach $63.5 Billion in 2026 at a CAGR of 18.2%,* Globe Newswire (Sept. 6, 2022), *https://www.globenewswire.com/en/news-release/2022/09/06/2510235/28124/en/Genomics-Global-Market-to-Reach-63-5-Billion-in-2026-at-a-CAGR-of-18-2.html* [*https://perma.cc/SUV8-VVMK*]; Grand View Research, Report ID No. 978–1–68038–299–0, *Biometric Technology Market Size, Share & Trends Analysis Report, 2023–2030* (2023), *https://www.grandviewresearch.com/industry-analysis/biometrics-industry* [*https://perma.cc/KN36-3KZW*]; Grand View Research, Report ID No. GVR–2–68038–401–7, *Location Intelligence Market Size, Share & Trends Analysis Report, 2024–2030* (2024), *https://www.grandviewresearch.com/industry-analysis/location-intelligence-market* [*https://perma.cc/WS6U-2324*].

v. Total Estimated Value of Lost and Forgone Transactions

To reiterate, U.S. exports of genomic, biometric, and location data to China and Russia totaled approximately $361 million in 2022. Some of these exports may have been for beneficial uses, such as consumer-choice improvement; effective medical responses; and increased knowledge of patterns of consumption, commerce, transportation, traffic, information/news transmission, nutrition, and health. The Department's estimates of the value of lost transactions do not include the potential value of any lost positive externalities to U.S. residents. The estimated annual value of lost or forgone transactions is presented in Table VII–10 of this preamble.

TABLE VII–10—ESTIMATED ANNUAL VALUE OF LOST TRANSACTIONS: GENOMIC, BIOMETRIC, AND LOCATION DATA

[In millions of 2022 dollars]

Country of concern	Value of forgone transactions
China	$267
Russia	94
Total	361

Source: Department of Justice estimates based on market research data from U.S.-based company, including: *Genomics Global Market to Reach $63.5 Billion in 2026 at a CAGR of 18.2%,* Globe Newswire *(Sept. 6, 2022), https://www.globenewswire.com/en/news-release/2022/09/06/2510235/28124/en/Genomics-Global-Market-to-Reach-63-5-Billion-in-2026-at-a-CAGR-of-18-2.html* [*https://perma.cc/SUV8-VVMK*]; Grand View Research, Report ID No. 978–1–68038–299–0, *Biometric Technology Market Size, Share & Trends Analysis Report, 2023–2030* (2023), *https://www.grandviewresearch.com/industry-analysis/biometrics-industry* [*https://perma.cc/KN36-3KZW*]; Grand View Research, Report ID No. GVR–2–68038–401–7, *Location Intelligence Market Size, Share & Trends Analysis Report, 2024–2030* (2024), *https://www.grandviewresearch.com/industry-analysis/location-intelligence-market* [*https://perma.cc/WS6U-2324*].

The Department welcomes comments on the use of this data and on any alternative or additional data that could also be employed. The Department reiterates the following limitations on these estimates, described in further detail in the analysis above:

1. The estimate assumes that the U.S. share of the global market value for location data is the same as the U.S. share of the global market value for genomic and biometric technology.
2. The export share of each of these respective U.S. markets is assumed to be the same as the share of revenue of U.S. data-brokerage companies that comes from international sales, which is 30 percent.
3. The estimate assumes that the database (and other information) services category of BEA's data includes most data brokers.
4. The estimate uses the share of U.S. exports of database and other information services that go to China and Russia to estimate the share of U.S. exports of genomic, biometric, and location data that go to China and Russia.
5. The Department assumes that the annual economic value of lost and forgone transactions would be equal to the value of all U.S. exports of biometric, location, and genomic data to China and Russia.

vi. Alternative Methodology for Estimating the Value of Lost and Forgone Transactions

An alternative estimate of the value of U.S. exports to China and Russia for this analysis can be derived from BEA data on the value of U.S. exports of database and other information services. As shown in the bottom of Table VII–7 of this preamble, BEA's estimates for 2023 were $318 million for China and $32 million for Russia.

Given the rapid growth of Chinese exports, the Department projected the 2023 BEA estimate forward to 2024. Based on the growth rates of U.S. exports of information services to China between 2006 and 2023,[509] using an annual growth rate of 5 percent for China [510] would increase BEA's $318 million estimate for 2023 to $334 million for 2024.

The Department's alternative estimates for the value of lost transactions are $334 million in forgone exports of information services to China and $32 million in foregone exports of information services to Russia, as shown in Table VII–11 of this preamble.

[509] U.S. Bureau of Econ. Analysis, *Table 2.3. U.S. Trade in Services, by Country or Affiliation and by Type of Service,* International Transactions, International Services, and International Investment Position Tables, *https://apps.bea.gov/iTable/?reqid=62&step=9&isuri=1&product=4#eyJhcHBpZCI6NjIsInN0ZXBzIjpbMSw5LDEwLDcsN10sImRhdGEiOltbInByb2R1Y3QiLCI0Il0sWyJUYWJsZUxpc3QiLCIzMDU4MyJdLFsiVGFibGVMaXN0U2Vjb25kYXJ5IiwiMzA2NTYiXSxbIkZpbHRlcl8jMSIsWyIxIiwiMiIsIjMiLCI0IiwiNSIsIjYiLCI3IiwiOCIsIjkiLCIxMCIsIjExIiwiMTIiLCIxMyIsIjE0IiwiMTUiLCIxNiIsIjE3IiwiMTgiXV0sWyJGaWx0ZXJfIzIiLFsiMjgiLCI3MyJdXSxbIkZpbHRlcl8jYIsWyIxIiwiNTUiLCI2MSIsIjYzIl1dLFsiUiLFsiMCJdXV19* [*https://perma.cc/7USS-P3PL*].

[510] Chu Daye, *China Achieves 5.2% GDP Growth in 2023,* Global Times (Jan. 17, 2024), *https://www.globaltimes.cn/page/202401/1305571.shtml* [*https://perma.cc/3NGJ-RXZ7*].

TABLE VII–11—ESTIMATES OF THE ANNUAL VALUE OF LOST TRANSACTIONS USING ALTERNATIVE METHODOLOGY

[In millions of 2022 dollars]

Country of concern	Estimated value of U.S. exports of data and information services
China	$334
Russia	32
Total	366

Source: U.S. Bureau of Econ. Analysis, *Table 2.3. U.S. Trade in Services, by Country or Affiliation and by Type of Service,* International Transactions, International Services, and International Investment Position Tables, *https://apps.bea.gov/iTable/?reqid=62&step=9&isuri=1&product=4#eyJhcHBpZCI6NjIsInN0ZXBzIjpbMSw5LDEwLDcsN10sImRhdGEiOltbInByb2R1Y3QiLCI0Il0sWyJUYWJsZUxpc3QiLCIzMDU4MyJdLFsiVGFibGVMaXN0U2Vjb25kYXJ5IiwiMzA2NTYiXSxbIkZpbHRlcl8jMSIsWyIxIiwiMiIsIjMiLCI0IiwiNSIsIjYiLCI3IiwiOCIsIjkiLCIxMCIsIjExIiwiMTIiLCIxMyIsIjE0IiwiMTUiLCIxNiIsIjE3IiwiMTgiXV0sWyJGaWx0ZXJfIzIiLFsiMjgiLCI3MyJdXSxbIkZpbHRlcl8jMyIsWyIxIiwiNTUiLCI2MSIsIjYzII1dLFsiRmlsdGVyXyM0IixbIjAiXV0sWyJGaWx0ZXJfIzUiLFsiMCJdXV19* [*https://perma.cc/7USS-P3PL*].

Under this alternative methodology, the Department's estimate of the economic value of transactions lost due to the proposed rule is $366 million per year (Table VII–11 of this preamble), compared with the $361 million estimate reached in the main analysis (Table VII–10 of this preamble).

The alternative methodology may overestimate the annual value of lost transactions, since the BEA category for the Database and Other Information Services may include many kinds of data that are explicitly excluded from regulation under the proposed rule (such as web-browser history and other expressive data).[511] The comparability of the main and alternative methodologies suggests that the main estimate of $361 million may underestimate the annual value of lost transactions because it does not include personal financial data or health records. With these disparities in mind, we are estimating the value of lost transactions at the midpoint of these estimates, $364 million, and solicit comments on this total.

The Department estimates that the economic value of lost or forgone transactions would be minimal for firms not engaged in data brokerage (*i.e.,* for restricted transactions). In other words, the Department assumes that firms not engaged in data brokerage would bear minimal economic costs beyond those that may be associated with implementing and maintaining a risk-based compliance program (as described in § 202.302 of the proposed rule). For example, the Department assumes that the small number of U.S.-based firms currently using Chinese cloud-service providers to store prohibited or restricted data would be able to switch to another cloud service provider at low or no cost, given that Chinese cloud-service providers constitute only a tiny fraction of the cloud market for U.S.-based firms. The Department assumes that the other five countries of interest do not sell cloud services of any significant value to the United States.[512]

b. Security Costs

Data security is an important aspect of protecting government-related data or bulk U.S. sensitive personal data from being improperly accessed by foreign adversaries or in ways that could pose a threat to national security. The proposed rule incorporates by reference proposed security requirements that have been developed by DHS through CISA, which represent conditions that businesses must meet to engage in restricted transactions. These security requirements are intended to address national security and foreign-policy threats that arise when countries of concern and covered persons access government-related data or bulk U.S. sensitive personal data that may be implicated by the categories of restricted transactions. Specifically, the proposed rule would prohibit U.S. persons from engaging in transactions unless they comply with three categories of requirements, the first two of which are addressed in the proposed security requirements, which are proposed to be incorporated by reference:

1. Organizational and system-level requirements for instituting cybersecurity policies, practices, and requirements for any covered system (which CISA proposes to define as a specific type of information system that is used to conduct a number of activities related to covered data as part of a restricted transaction).

2. Data-level requirements using any combination of the following capabilities necessary to prevent access to covered data by covered persons or countries of concern:

a. Data minimization and data masking;

b. Encryption;

c. Privacy-enhancing technologies; and

d. Denial of access.

3. Compliance-Related Requirements for Independent Testing and Auditing

These requirements would impose new costs on firms to the extent that they are not already voluntarily meeting such requirements. Any additional costs may be offset by reducing cyber incidents and their associated costs. The Department estimates the new cybersecurity-related costs imposed on affected firms by analyzing the costs that companies at different sizes and levels of technological maturity face when implementing existing security standards and frameworks of similar scope.

i. Similar Security Standards and Frameworks

The proposed rule would create cybersecurity standards that are based on, and thus overlap with, several similar, widely used cybersecurity standards or frameworks. Currently, firms engaged in transactions that are proposed to be restricted transactions are encouraged—but generally not explicitly required—to comply with existing Federal cybersecurity standards or frameworks. Given the similarities between the proposed rule's security requirements and existing cybersecurity standards and frameworks, the costs of complying with one of the existing, commonly implemented sets of cybersecurity standards or frameworks are likely similar to the costs that would be incurred by businesses to comply

[511] Sherman, *supra* note 6.

[512] David McCabe, *China's Cloud Computing Firms Raise Concern for U.S.,* N.Y. Times (June 21, 2023), *https://www.nytimes.com/2023/06/21/technology/china-cloud-computing-concern.html* [*https://perma.cc/4CQJ-F6GJ*].

with the proposed rule. Furthermore, such costs will be offset because, as commenters generally agreed, most companies will already have foundational baseline security requirements in place.

As required by the Order, the security requirements for firms engaged in restricted transactions are based on the National Institute of Standards and Technology (''NIST'') Cybersecurity Framework (''CSF'') [513] and the NIST Privacy Framework (''PF'').[514] CISA has also leveraged existing performance goals, guidance, practices, and controls, including the CISA Cross-Sector Cybersecurity Performance Goals (''CPGs''),[515] which are themselves based on the NIST CSF and PF.

The CPGs, NIST CSF, and NIST PF are sets of recommendations, based on current best practices, that companies can voluntarily follow. The CPGs are themselves mapped to the CSF. In its proposed security requirements, CISA has included mapping to the CPGs and NIST CSF and PF, as applicable. Furthermore, the CSF aligns its requirements with other similar standards that are commonly used in industry, including NIST SP 800–53 and International Organization for Standardization/International Electrotechnical Commission (''ISO'')/(''IEC'') 27001:2013. The ISO/IEC 27001:2013 standard, unlike the CISA and NIST frameworks, has a more formal certification process and has granted certificates to 48,671 companies globally and 1,898 companies in the United States.[516] Finally, NIST SP 800–171 rev.3,[517] a common security framework, lays out security standards for firms handling controlled unclassified information, while the Department of Defense's Cybersecurity Maturity Model Certification (''CMMC'') program [518] includes the NIST SP 800–171 requirements but with a more formal auditing and certification process.

ii. Current Industry Compliance Level

The majority of firms affected by the proposed rule likely already comply with some portion of the security requirements in the proposed rule. The level of existing adherence to the proposed security requirements for the average U.S. company would vary significantly based on each firm's size, industry, existing regulatory landscape, technological maturity, and internalized priorities.[519] Given the high degree of overlap between the DHS draft security requirements and existing standards and frameworks discussed below, it is possible that the level of existing compliance among affected firms will be high.

One survey of business expenditures on cybersecurity conducted by IANS Research indicates that such spending can vary depending on industry and business size. According to this survey, the average firm spent nearly 10 percent of its IT budget on cybersecurity, with firms in industries like technology, healthcare, and business services spending the highest proportion at over 13 percent.[520] Furthermore, in the same report, an analysis of firm size found that smaller businesses spend the highest proportion of their IT budgets on cybersecurity.[521] While it is possible that companies with larger expenditures on cybersecurity would be closer to compliance with the proposed rule, it is difficult to determine with the available data the extent to which companies are using their cybersecurity budgets to keep up with evolving best practices and maintain the capabilities required by the proposed security requirements.

The level of technological and cybersecurity maturity also varies significantly, even among larger firms. Recent data indicates that there is great variability in cybersecurity practice sophistication and maturity. In 2023, Deloitte conducted a survey of cyber decision makers at firms around the world with at least 1,000 employees and $500 million in annual revenue. The Deloitte study determined that of these organizations, 38 percent had low cyber maturity (as defined in the study), 41 percent had medium cyber maturity, and 21 percent had high cyber maturity.[522] Another survey of IT professionals found that 45 percent of firms did not have a designated Chief Information Security Officer, which would make them noncompliant with the proposed security requirements.[523]

Furthermore, research suggests that the cost of cybersecurity activities can vary based on factors such as the size of the company, the cybersecurity capabilities required, and whether those capabilities are developed in house or by contracting with third parties. Additionally, the Center for internet Security provided high and low estimates of cybersecurity budgets based on company size, with an average estimate of $22,000 for a small firm (1 to 10 employees) and about $800,000 for a large firm (100 to 999 employees).[524]

iii. Costs of Compliance

Regarding the cost of compliance, the Department assumes that most affected companies will not have to build cybersecurity capabilities from the ground up to meet the requirements of the proposed rule. Given that most firms will have existing cybersecurity protections in place, a more realistic approach to calculating the potential cost of the proposed rule would be to consider the additional expenditures that a company would have to make to increase its cybersecurity standards. The Department assumes, based on the

---

[513] Nat'l Inst. of Standards & Tech., *Framework for Improving Critical Infrastructure Cybersecurity* (v. 1.1, Apr. 16, 2018), *https://doi.org/10.6028/NIST.CSWP.04162018* [*https://perma.cc/2FKZ-3PAT*].

[514] Nat'l Inst. of Standards & Tech., *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management* (v. 1.0, Jan. 16, 2020), *https://doi.org/10.6028/NIST.CSWP.01162020* [*https://perma.cc/36SC-VZXN*].

[515] Cybersec. & Infrastructure Sec. Agency, *Cross-Sector Cybersecurity Performance Goals: March 2023 Update* (2023), *https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_report_v1.0.1_final.pdf* [*https://perma.cc/4YRS-Z9UJ*].

[516] Int'l Org. for Standardization, *ISO/IEC 27001:2013&2022 Information Technology—Security Techniques—Information Security Management Systems—Requirements,* 1. ISO Survey 2023 Results—Number of Certificates and Sites per Country and the Number of Sectors Overall (Sept. 18, 2024), *https://www.iso.org/committee/54998.html?t=KomURwikWDLiuB1P1c7SjLMLEAgXOA7emZHKGWyn8f3KQUTU3m287NxnpA3DIuxm&view=documents* [*https://perma.cc/L43C-MVY8*] (click ''1. ISO Survey 2023 results—Number of certificates and sites per country and the number of sectors overall'' to download spreadsheet; then open tab titled ''ISO IEC 27001'' in that file).

[517] Ron Ross & Victoria Pillitteri, Nat'l Inst. of Standards & Tech., NIST SP 800–171r3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations,* Nat'l Inst. of Standards & Tech. (2024), *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r3.pdf* [*https://perma.cc/ER88-7Y8F*].

[518] U.S. Dep't of Def., Office of the Undersecretary of Defense for Acquisition & Sustainment, *Cybersecurity Maturity Model Certification (CMMC) Model Overview Version 2.0* (2021), *https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview_V2.0_FINAL2_20211202_508.pdf* [*https://perma.cc/2HAM-92TJ*].

[519] Deloitte, *2023 Global Future of Cyber Survey* (2023), *https://www.deloitte.com/content/dam/assets-shared/docs/services/risk-advisory/2023/gx-deloitte_future_of_cyber_2023.pdf* [*https://perma.cc/B9E3-QNRW*].

[520] IANS Research, *Benchmark Insights: Security Budget Benchmark Summary Report* 4 (2022), *https://cdn.iansresearch.com/Files/Marketing/IANSResearch-2022SecurityBudgetBenchmarkSummaryReport.pdf* [*https://perma.cc/B9SE-4YS5*].

[521] *Id.*

[522] Deloitte, supra note 519, at 14.

[523] Navisite, *The State of Cybersecurity Leadership and Readiness, Fall 2021* (2021), at 4, *https://lp.navisite.com/l/824543/2023-05-19/3733vx/824543/1684513240bPrtcWBS/state_of_cybersecurity_leadership_and_readiness_report.pdf* [*https://perma.cc/6VQG-VGZG*].

[524] The average budget estimates for the small and large firms were calculated by averaging the high and low estimates from the relevant size category. Ctr. for internet Sec., *The Cost of Cyber Defense: CIS Controls Implementation Group 1,* at 8 (v. 1.0, 2023), *https://learn.cisecurity.org/l/799323/2023-08-02/4t3qkj/799323/1694810927NC0iZQGR/CIS_Controls__Cost_of_Cyber_Defense__2023_08.pdf* [*https://perma.cc/C46G-EZFR*].

design of the proposed rule, that added cybersecurity compliance costs will closely mirror the costs that companies face when complying with similar or more onerous/prescriptive standards, such as NIST 800–171, NIST 800–53, ISO/IEC 27001, and the CMMC program, providing a helpful tool to estimate the added compliance costs associated with the data security requirements, though such estimates may be conservative. Furthermore, since some firms may already clearly be in voluntary compliance with more stringent standards than the proposed security standards, which would allow them to forgo some of the following steps, some of the costs may not be incurred by all firms.

The first step that most firms engaging in restricted transactions will take toward compliance is completing an assessment of their current capabilities and shortcomings. For example, it would cost a small to medium-sized firm that is working toward compliance with NIST 800–171 and NIST 800–53 around $30,000 to $35,000 to build in-house assessment capabilities.[525] Along the same lines, another source estimates that an assessment for a CMMC certification for a firm with 250 employees could cost up to $35,000.[526] For the initial assessment stage of the ISO/IEC 27001 certification process, a small business would expect to spend $25,000 to $40,000 to complete the process internally and around $30,000 to hire a consultant.[527] However, a company with more complicated compliance issues could expect to pay as much as $130,000 for the consulting and assessment.[528] Thus, the Department finds that an assessment will cost between $25,000 and $130,000 for most firms, depending on the scale of the compliance needs involved.

The next step in the compliance process is remediating the issues found in the initial assessment. It is likely that remediation would involve a combination of fixed and recurring costs. One-time remediation costs could involve revising security policies or patching vulnerabilities in covered systems, while recurring costs could include subscriptions to services that provide data encryption, multifactor authentication, or password management services, as well as costs associated with maintaining access controls or required documentation. Estimates for remediation costs for NIST 800–171 compliance range between $35,000 and $115,000.[529] Another estimate suggests that midsized companies with lower levels of technological maturity can expect to pay approximately $100,000 to correct any compliance issues.[530]

In accordance with the security requirements with which U.S. persons engaged in restricted transactions must comply under the proposed rule, every firm, regardless of its initial compliance level, will need to annually verify its compliance through audits and testing. This is a common cost that firms incur to comply with existing frameworks or standards. For a small company with 50 employees, the annual recertification audit for ISO/IEC 27001 compliance costs an estimated $6,000 to $7,500.[531] The continuous monitoring costs associated with NIST 800–171 compliance for small businesses are estimated to be around $6,500 to $13,000.[532] However, annual surveillance audits to ensure compliance with ISO/IEC 27001 standards can cost as much as $40,000.[533]

Table VII–12 of this preamble summarizes the high and low estimates for the costs—both one-time and ongoing—that an average U.S. company engaged in restricted transactions may face under the proposed rule. A firm may find itself in the higher-cost category based on either greater size and complexity or a lower level of technological maturity. For this analysis, it is assumed that even firms in the low-cost scenario will have added costs in each category. Furthermore, based on the Department's experience, half of the added one-time remediation costs in both the high and low estimates are assumed to recur annually. Finally, for the added training costs, the low estimate was taken from the small business low-cost figure in a report by the Center for internet Security, and the high estimate was taken from the midsized business high-cost figure in the same report.[534]

TABLE VII–12—COSTS OF COMPLYING WITH THE PROPOSED SECURITY REQUIREMENTS

Category	Cost—Low	Cost—High	Type
Initial Assessment	$25,000	$130,000	One-time.
Remediation	35,000	115,000	One-time.
Ongoing Remediation	17,500	57,500	Annually recurring.
Compliance Audits	6,000	40,000	Annually recurring.
Training	120	3,660	Annually recurring.

c. Costs Associated With Compliance Program: Due Diligence, Recordkeeping, and Auditing

In addition to security requirements, the proposed rule also introduces affirmative due diligence, recordkeeping, affirmative reporting, and auditing requirements as conditions of a license or for U.S. persons engaged in restricted transactions, each of which would likely impose added costs. In this section, the Department estimates costs for affirmative due diligence, recordkeeping, and auditing for firms engaged in licensed or restricted transactions.

The compliance program for affirmative due diligence,

[525] *Estimated Costs Associated with NIST 800–53 and NIST 800–171 Security Risk Assessments,* GoldSky Security (Apr. 29, 2021), *https://www.goldskysecurity.com/estimated-costs-associated-with-nist-800-53-and-nist-800-171-security-risk-assessments/* [*https://perma.cc/87V6-FZ4N*].

[526] *CMMC Certification Cost: The Price of Compliance,* Cuick Trac, *https://www.cuicktrac.com/blog/cmmc-certification-cost/* [*https://perma.cc/KR79-AWLA*].

[527] *How Much Does ISO 27001 Certification Cost?,* OneTrust: Blog (Sept. 21, 2022), *https://www.onetrust.com/blog/iso-27001-certification/* [*https://perma.cc/G5UU-P62E*].

[528] *Cost of Compliance with CMMC and NIST–171,* Hyper Vigilance, *https://blog.hypervigilance.com/cost-of-cmmc-nist-compliance* [*https://perma.cc/PF8Z-QVTM*].

[529] *Navigate NIST 800–171 with Confidence,* Fortified Services, *https://nist171.fortifiedservices.com/* [*https://perma.cc/K92U-UCAY*]; *Cost of Compliance with CMMC and NIST–171, supra* note 528.

[530] *Cost of Compliance with CMMC and NIST–171, supra* note 528.

[531] *How Much Does ISO 27001 Certification Cost?, supra* note 527.

[532] *Navigate NIST 800–171 with Confidence, supra* note 529.

[533] Srividhya Karthik, *ISO 27001 Certification Cost: Plan Your Compliance Budget Better,* Sprinto (Mar. 1, 2024), *https://sprinto.com/blog/iso-27001-certification-cost/* [*https://perma.cc/YP75-YW6G*].

[534] Ctr. for internet Sec., *supra* note 524, at 22.

recordkeeping, and auditing would consist partly of risk-based procedures for verifying the data flows involved in any restricted transaction. Further requirements would include a policy describing the compliance program and process, a policy describing the implementation of any applicable security requirements or other conditions, annual certification of such compliance policies, maintenance records documenting the due diligence performed in implementing the compliance policy with respect to data transactions, and an annual certification of the completeness and accuracy of the records documenting due diligence as supported by an audit.

With regard to due diligence, recordkeeping, and auditing costs for U.S. companies, precise numbers on the number of affected firms, their sizes, and per-company or per-transaction costs are very difficult to estimate. Further, the compliance costs for firms that have established programs relative to existing Federal and State regulations may be minimal, as their compliance approach can be modified at low or no cost to address the proposed security requirements, whereas firms without such compliance programs would likely incur higher costs.

In particular, many firms may have existing compliance programs targeted at three notable provisions that were passed and implemented in recent years: the California Consumer Privacy Act of 2018 (''CCPA'') [535] the EU's General Data Protection Regulation (''GDPR''),[536] and the APEC CBPR.[537] More than 10 other U.S. States have also recently passed data privacy legislation, and many others are considering such laws.[538] Due to these laws and existing Federal export-related regulations, it is possible that some expected due diligence costs imposed by the proposed rule may have already been incurred by affected businesses. However, given that the definitions under the proposed rule do not fully align with the definitions used in these frameworks, there are likely to be separate due diligence costs.

The Department has estimated upper- and lower-bound costs to firms from the proposed rule related to due diligence, recordkeeping, and auditing based on our analysis of the literature regarding the CCPA, GDPR, and other data privacy rules and related research. These upper- and lower-bound estimates and the supporting literature are discussed in this part VII.A.8.c of this preamble. In summary, part VII.A.8.c.i of this preamble estimates that Know Your Customer/Know Your Vendor (''KYC''/''KYV'') costs for verifying one's business and its executives are between $150 (lower bound) and $4,230 (upper bound). In addition, parts VII.A.8.c.ii through VII.A.8.c.iv of this preamble estimate that the combined annual recordkeeping and auditing costs per firm are between a lower bound of $1,260 ($300 for auditing + $960 for recordkeeping) and an upper bound of $232,500 ($7,500 for auditing + $225,000 for recordkeeping). These estimates are based on the Department's analysis, but could be different depending on industry and context. The Department welcomes additional input from stakeholders on this point.

i. Due Diligence Costs

The proposed rule requires entities engaged in restricted transactions to perform due diligence that includes KYC/KYV activities, which may involve verifications to confirm the legitimacy and eligibility of customers and vendors. Costs would generally be incurred one time per customer or vendor, but they could be repetitive if there is reason to believe that a customer or vendor's legitimacy or eligibility has changed. The Department estimates the due diligence (*i.e.,* KYC/KYV) costs for verifying one business and its executives at between $150 (lower bound) and $4,230 (upper bound).

The upper-bound estimate assumes that the background check costs for one customer or vendor business would include a background check for the business and three background checks for executives residing outside the United States. The Department estimates an upper-bound cost of $1,200 per business background check based on a study showing an upper-bound range of more than $1,000 for a due diligence background check of a business.[539] The Department estimates an upper-bound cost of $1,010 per executive background check based on the highest cost for a background check of an executive residing in a country of concern (which is associated with Venezuela) from Table VII–13 of this preamble.[540] Therefore, the upper-bound background check costs for one customer business with three executives could be as high as $4,230 ($1,200 per business [541] + ($1,010 per executive [542] * 3)).

One company, Global Background Screening, charges $150 to $250 for business background checks, with the higher end for businesses headquartered outside the United States.[543] These business background checks include documentation on directorship, financials, registration, judgments, liens, bankruptcies, and credit risk.[544] Screenings for firm executives appear to be separate costs, which vary by country of residence and type of background check, as summarized in Table VII–13 of this preamble. Countries identified in the proposed rule as countries of concern (*see* § 202.209) are included in Table VII–13 of this preamble where sufficient data is available. Santoni also advertises due diligence business background checks, which appear to include foreign firms and officers, ranging from $395 to more than $1,000.[545]

[535] California Consumer Privacy Act of 2018, *supra* note 28.

[536] Regulation (EU) 2016/679, *supra* note 28.

[537] Asia-Pac. Econ. Coop., *APEC Cross-Border Privacy Enforcement Arrangement (CPEA)* (Feb. 2024), *https://www.apec.org/groups/committee-on-trade-and-investment/digital-economy-steering-group/cross-border-privacy-enforcement-arrangement#* [*https://perma.cc/GRA3-8UQX*].

[538] *US State Privacy Legislation Tracker,* Int'l Ass'n of Privacy Pros. (July 22, 2024), *https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf* [*https://perma.cc/WF3A-PJ5K*].

[539] Tim Santoni, *So What's the Difference Between Background Checks and Investigations?,* Santoni, *https://santoniservices.com/whats-new-at-santoni/whats-the-difference-between-background-checks-and-investigations/* [*https://perma.cc/WM9X-5YMY*].

[540] *International Screening Checkout Portal,* Global Background Screening, *https://www.globalbackgroundscreening.com/online-background-check/International-Employee-Screening-Select-Country-For-Pricing-p303546142* [*https://perma.cc/3AUN-84R4*] (select most expensive options for all Venezuelan searches and verifications from dropdowns).

[541] Santoni, *supra* note 539 (estimating that a due diligence background check for a business may cost over $1,000).

[542] *International Screening Checkout Portal, supra* note 540.

[543] *Background Check on a Business,* Global Background Screening, *https://www.globalbackgroundscreening.com/online-background-check/background-check-on-a-business-p316742635* [*https://perma.cc/3AUN-84R4*].

[544] Carlos Crameri, *Business Credit Reports for Informed Decision-Making,* Global Background Screening (Mar. 21, 2023), *https://www.globalbackgroundscreening.com/online-background-check/BACKGROUND-CHECK-ON-A-BUSINESS-p316742635* [*https://perma.cc/QE6U-FFMR*]; for more detailed pricing, *see Background Check on a Business,* Global Background Screening, *https://www.globalbackgroundscreening.com/online-background-check/background-check-on-a-business-p316742635* [*https://perma.cc/3AUN-84R4*].

[545] Santoni, *supra* note 539.

TABLE VII–13—ESTIMATED INTERNATIONAL SCREENING COSTS FOR INDIVIDUALS BY COUNTRY OF RESIDENCE

Type of screening	China	Russia	Cuba	Venezuela	All nations low	All nations high
Criminal background	$80–$110	$129	$169	$135	$59	$260
Civil judgements	80	145	239	159	45	279
Identity verification	25	25	25	25	25	25
Bankruptcy records	50	.....	.....	188	23	188
Credit history	80	127	274	234	50	532
Employment verification	35–99	35–99	35–99	35–99	35	99
Education verification	35	35	35	35	35	35
Worldscan (global databases)	11–65	11–65	11–65	11–65	11	65
Social media scan	50–70	50–70	50–70	50–70	50	70
Totals	446–614	557–695	838–976	872–1,010	333	1,553

Source: *International Screening Checkout Portal,* Global Background Screening, *https://www.globalbackgroundscreening.com/online-background-check/International-Employee-Screening-Select-Country-For-Pricing-p303546142* (reflecting costs of services at the time the Department drafted the proposed rule).

The remainder of this section summarizes additional research on background check costs for foreign firms and for individuals residing outside the United States, which is broadly consistent with the Department's upper- and lower-bound estimates discussed so far in this section.

The U.S. International Trade Administration (''ITA'') provides basic background check and in-depth data on foreign firms to help U.S. companies determine the suitability of possible business partners. To be eligible for the service, companies must be export-ready and endeavoring to export goods or services of U.S. origin with at least 51-percent U.S. content. The ITA provides partial profiles that include general business information, background and product data, pertinent executives, reputation information, brief analysis of information collected, and identities of the references used. Fees for these partial profiles range from $150 to $450 depending on the size of the inquiring firm. Full business profiles add onsite visits and interviews of company executives, with costs ranging from $700 to $2,000. Costs could increase if ITA staff are required to travel more than 80 kilometers or 2 hours from an ITA office.[546]

Diligentia, Inc. categorizes background checks on individuals based on the thoroughness of the investigation. An individual or red flag investigation is designed to identify adverse issues predominantly via online searches, at a cost of $500 to $1,500. A professional background investigation is a more thorough review that adds onsite records depository visits and analysis of documents there, at a cost of $1,500 to $2,500. A comprehensive background investigation goes even further, with additional analyses, reviews of business interests, the use of other intelligence sources, financial investigation, and a credit history, at a cost of more than $2,500. This provider does not advertise a price difference between domestic and foreign background investigations.[547]

Checkr states that international background checks can range from $30 to $500, with their fees varying from $32 to $300 and covering more than 200 countries. Checkr asserts that a global background check may include searches for criminal history, watchlist posting, education/employment verification, and media checks.[548]

An ITA partial or full profile of foreign businesses would likely be preferable for U.S. companies due to the real or perceived credibility of a government agency and the comparatively reasonable costs. Accordingly, for verifying one business and its executives, the Department relied on ITA's pricing for the estimated lower-bound cost of $150.

The sources supporting our cost estimates do not discuss whether the costs include extensive investigations that involve foreign travel or contracting with third parties in foreign locations to perform onsite visits, inquiries, interviews, and other in-depth activities. The Department estimates that it is unlikely that firms would allocate resources for these kinds of investigations, particularly when the ITA service is available. However, some firms may not meet the ITA's eligibility criteria for their services. Thus, it is possible that KYC/KYV activities may need to be performed via a private vendor, such as one of the vendors just described. Again, based on the analysis, the Department estimates the due diligence costs for verifying one business and its executives at between $150 (lower bound) and $4,230 (upper bound).

These estimates are based on Department analysis but could be different depending on the industry and context. The DOJ welcomes additional input from stakeholders on this point.

ii. Recordkeeping Costs

The proposed rule's recordkeeping requirements would include generating or maintaining documents pertinent to various data transactions details, verifications of transaction partners, transactions agreements, licenses, exemptions, advisory opinions, annual due diligence certifications, and supporting documentation, as applicable. Data brokers incorporated in the United States market and sell data on individuals not only domestically but from many other countries;[549] for example, Acxiom markets data coverage for more than 62 countries.[550] Assuming that this data on foreign persons includes individuals protected by EU

[546] Int'l Trade Admin., *International Company Profile (Full and Partial), https://www.trade.gov/international-company-profile-0* [*https://perma.cc/N3PX-4DEZ*].

[547] Brian Willingham, *How Much Does a Background Investigation Cost?,* Diligentia Group (Apr. 23, 2024), *https://diligentiagroup.com/background-investigations/how-much-does-a-background-investigation-cost/* [*https://perma.cc/2RGF-LH5G*].

[548] *Simple, Transparent Pricing: Background Check Pricing for Businesses of All Sizes,* Checkr, *https://checkr.com/pricing?utm_medium=ppc&utm_source=google&utm_campaign=pricing_sitelink&utm_term=checkr&utm_campaign=FM_Brand_Search_LP_Control_1122&utm_source=google&utm_medium=ppc&utm_content=677534444565&_bm=p&_bn=g&device=c&utm_adgroup=Brand_Core&gad_source=1&gclid=Cj0KCQjwyL24BhCtARIsALo0fSAQPeVlfGXfAoN59kjZI4TEpIchvwY7u4ZdX3iPL0Sg8Z0_ZVLLjPwaApKyEALw_wcB* [*https://perma.cc/7U3R-T8R5*].

[549] Sherman, *supra* note 483.

[550] Acxiom LLC, *Global Data Navigator* (2018), *https://marketing.acxiom.com/rs/982-LRE-196/images/Acxiom%20Global%20Data.pdf* [*https://perma.cc/4NX5-M8P6*].

law, these data brokers are subject to the GDPR.

Since 2018, the GDPR has required all organizations that target or collect data relative to persons in the EU to abide by privacy and security standards outlined in that law. One of the seven data protection principles in the GDPR is accountability or due diligence. Accordingly, data controllers (*i.e.,* holders of data) must be able to demonstrate compliance relative to accountability by (1) designating data protection responsibilities as appropriate; (2) maintaining comprehensive records of collected data, its use, and those responsible for it; (3) training staff and executing technical and organizational security measures; (4) implementing contracts with third parties that process data on their behalf; and (5) appointing a data protection officer (if a public authority or regularly processing personal data on a large scale).[551] Thus, a portion of covered persons subject to the proposed rule are already complying with GDPR recordkeeping requirements and would arguably not incur the full magnitude of these new costs.

iii. Executive Order on Modernizing Regulatory Review Recordkeeping and Related Costs

As shown in the following analysis, the annual recordkeeping and related costs per firm are estimated to be between $960 (lower bound) and $225,000 (upper bound).

The Department calculates a lower-bound estimate of annual recordkeeping costs per firm by starting with the average annual incremental compliance costs/administrative burdens from the EU impact assessment of GDPR. According to the EU's impact assessment of the GDPR, average annual incremental compliance costs/administrative burdens for small and medium-sized enterprises (''SMEs'') [552] are approximately $9,624 (in 2024 dollars).[553] The Department assumes that the incremental recordkeeping costs of the proposed rule would only be about 10 percent of the estimated incremental annual costs for GDPR compliance. This assumption is based on the facts that the GDPR includes extensive recordkeeping requirements [554] and that many of the proposed rule's recordkeeping requirements are similar in scope to the obligations of existing data protection regulations.[555] Furthermore, the EU's impact assessment of the GDPR includes costs of compliance beyond recordkeeping costs. Based on these considerations and input from SMEs, the Department estimates that 1,400 small to medium-sized firms will incur recordkeeping costs of $960 per firm per year.

An upper-bound estimate of annual recordkeeping costs per firm is also based on estimates of company privacy protection annual costs, which for large firms were estimated at $4.5 million per firm.[556] The Department further estimates that the incremental recordkeeping costs of the proposed rule for large firms would be approximately 5 percent of the estimated annual costs for privacy protections. This assumption is based on the same factors as those described for the lower-bound annual recordkeeping cost estimate as well as the fact that the prior study included additional necessary costs (*e.g.,* IT upgrades) beyond recordkeeping alone. Further, the Department believes that larger firms predominantly have the added benefit of possessing additional sophistication in complying with existing data privacy and security regimes and already have significant compliance programs and mechanisms in place. Thus, based on this analysis and subject-matter expert input, the Department estimates that 100 firms will incur the higher recordkeeping costs of $225,000 per firm.

To provide context on these upper- and lower-bound recordkeeping costs, this section summarizes additional studies.

The CCPA mandated that businesses in California update privacy policies, develop mechanisms for providing notice to consumers when collecting personal information (''PI''), and adequately respond to consumer wishes regarding the handling of such data. The State of California Department of Justice, Office of the Attorney General's (''CDOJAG'') standardized regulatory impact assessment for the CCPA regulations estimated the following rule-imposed costs per firm: $959 in one-time operational costs (*e.g.,* establishing workflows/plans), $7,500 for technological systems development (assumed one-time), $615 per year for training, $984 per year to abide by record-keeping requirements (one data privacy professional at $61.50 per hour * 16 hours),[557] and $492 (assumed per year) to provide financial incentives or differential services/prices to promote non-discriminatory practices in their treatment of consumers exercising their CCPA rights. Apart from the $984 in compliance-related costs, the CDOJAG assumed that there were no incremental costs for collecting the information subject to the CCPA's recordkeeping requirement, as affected businesses likely already had mature mechanisms for identifying, processing, and analyzing PI from their data-mapping and consumer response practices. The CDOJAG's total estimated costs per firm to comply with the CCPA were about $29,000 ($2,900 annually) for the period from 2020 to 2030.[558]

Christensen et al. estimated GDPR compliance costs at between $5,065 and $12,157 (2024 dollars) [559] per year per SME, which represents a 16- to 40-percent increase in annual IT budgets. These presumably would align with the aforementioned GDPR accountability

[551] Ben Wolford, *What Is GDPR, the EU's New Data Protection Law?,* GDPR.eu, *https://gdpr.eu/what-is-gdpr/* [*https://perma.cc/ECS2-P67N*].

[552] According to the European Commission, SMEs consist of the following company types: medium with <250 employees, ≤€50 million turnover, or a balance sheet total ≤€43 million; small with <50 employees, ≤€10 million turnover, or a balance sheet total ≤€10 million; and micro with <10 employees, ≤€2 million turnover, or a balance sheet total ≤€2 million. *See* European Comm'n, *SME definition,* Internal Market, Industry, Entrepreneurship and SMEs, *https://single-market-economy.ec.europa.eu/smes/sme-definition_en* [*https://perma.cc/N4UX-WV5V*].

[553] €5.258 billion/926,272 active cross-border firms = €5,676 per SME per year = $7,068 at July 2012 average exchange rate (€1.00 = $1.24). European Comm'n, Doc. 52012SC0072, *Commission Staff Working Paper Impact Assessment,* Annex 9 (Jan. 25, 2012), *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52012SC0072&qid=1713360200812* [*https://perma.cc/W3FZ-GQ9Z*].

[554] Regulation (EU) 2016/679, *supra* note 28, at art. 30.

[555] *Id.; see infra* note 557 and accompanying text.

[556] This cost figure was converted into 2024 dollars. Cisco, Data Privacy Benchmark Study, *Forged by the Pandemic: The Age of Privacy* 9 (2021), *https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2021.pdf* [*https://perma.cc/6UTB-48C3*]. Note that large firms were assumed to be the complement of the aforementioned small to medium-sized firms.

[557] Off. of Att'y Gen., Cal. Dep't of Just, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations* 24 (2019), *https://dof.ca.gov/wp-content/uploads/sites/352/Forecasting/Economics/Documents/CCPA_Regulations-SRIA-DOF.pdf* [*https://perma.cc/5J5S-7DNA*]. The record-keeping requirements contained in the CCPA consist mainly of documenting business practices when processing consumer requests on how their particular data is handled. Businesses are required to compile metrics on these requests and their responses. These metrics include the number of requests to know, delete, and opt out that were received, complied with, and denied.

[558] *Id.* Ten-year costs per firm: $959 + $7,500 + $6,150 + $9,840 ($61.50 × 16 hrs. × 10 yrs.) + $4,920 = $29,369 for 10 years (*Id.,* at 24–28).

[559] €3,000 ($3,720 in 2012 dollars) to €7,200 ($8,929 in 2012 dollars) per SME per year; Laurits R. Christensen et al., *The Impact of the Data Protection Regulation in the E.U.* (Feb. 13, 2013), *https://www.analysisgroup.com/globalassets/insights/publishing/2013_data_protection_reg_in_eu_christensen_rafert_etal.pdf* [*https://perma.cc/4K3B-DF2R*].

elements identified by Wolford,[560] which are generally consistent with those of the proposed rule.

A 2018 International Association of Privacy Professionals and Ernst & Young (''IAPP''/''EY'') study/survey identified much higher average expected spending of about $3 million per firm on GDPR compliance, or $300,000 annually if assumed over 10 years. This included $1,276,000 already spent, another $822,000 expected for adaptation of products and services, and $989,000 for other adaptation activities. However, the average annual costs per firm due to GDPR were unclear based on the IAPP/EY 2018 and 2019 surveys. Company annual mean and median privacy-related spending ranged from $128 to $147 on a per-employee basis. Survey respondents were a mix of company sizes ranging from under 100 employees to more than 75,000.[561]

A 2021 Cisco annual global survey of all major industries found that annual privacy budgets doubled from the previous year to an average of $2.4 million (with smaller firms at a lower end of $1.6 million and larger firms at an upper end of $3.7 million, as reported in 2020).[562] This average figure of $2.4 million is comparable to a high-end estimate found in another study that aimed to project the costs to businesses incurred by possible Florida consumer privacy legislation; that study had a lower-bound estimate of about $733,000 in one-time costs per firm and subsequent ongoing annual costs ranging from about $542,000 to $1.5 million.[563] Organizations may spend an average of about $1,406 per subject rights request by consumers pursuant to privacy regulations.[564] According to one estimate, data processing agreements may have an average cost of $785.[565] Though privacy budgets, including some of their underlying elements, are different in scope and detail from the proposed rule they nonetheless have relevance for estimating the costs of the proposed rule as these budgets often serve similar objectives and require companies to undertake similar processes to protect sensitive data.

The relatively new APEC CBPR is a voluntary accountability framework regulating data transfers between member nations that is somewhat similar to the EU's GDPR, but based on Organisation for Economic Co-operation and Development (''OECD'') privacy principles.[566] In the United States, APEC CBPR annual certification costs range from $15,000 to $40,000.[567] The APEC CBPR's data security [568] due diligence mechanism is another requirement with which firms may already be complying and thus could reduce incremental costs of the proposed rule due to comparable or related requirements.

In summary, available sources show variations regarding the compliance costs for data privacy and cybersecurity regulations specific to recordkeeping. The Department estimates that it is very likely that incremental recordkeeping costs for at least some firms impacted by the proposed rule are zero, as the CDOJAG discussed in its cost estimates for the CCPA. Conversely, the possibility exists that larger firms have not been subject to the EU's GDPR and would be impacted by the proposed rule, resulting in their incurring some portion of the $4.5 million in 2024 in estimated annual recordkeeping costs documented by Cisco for such firms.[569] These ranges, along with the other data and analysis discussed throughout this subpart, were taken into consideration for the calculations of the proposed rule's average annual lower- and upper-bound costs per firm of $960 and $225,000. Part VII.F of this preamble estimates that costs due to the proposed annual reporting requirements for certain categories of U.S. persons engaged in certain subsets of restricted transactions would range from $821,100 (lower bound) to $1,642,200 (upper bound).

iv. Auditing Costs

As shown in the following analysis, annual auditing costs per firm are estimated to be between $300 (lower bound) and $7,500 (upper bound).

Auditing costs for restricted transactions would be incurred in the form of independent examinations to support the due diligence certifications. TrustNet offers services to help firms determine their compliance with the CCPA. One such service is a CCPA gap assessment, which covers scope, project management, risk assessment, controls identification, testing/analysis, remediation roadmap, and reporting. The cost of this service starts at $10,000. TrustNet also offers a CCPA compliance assessment with costs starting at $15,000, which covers similar elements.[570]

According to Neumetric, a cybersecurity products and services company, GDPR accreditation or certification is not offered by the EU or any of its member states. Firms do not need to certify that they are GDPR compliant; however, there are third-party certification bodies/consultants that offer GDPR certification services for consultant fees ranging from $3,000 to $11,000, on average.[571] This does not include internal costs to prepare for certification or other prerequisites for obtaining ISO/IEC 27001 and ISO 27701 certification, which could cost between $1,000 and $4,000.[572] Another source estimated that costs for GDPR certification range from about $5,000 to $20,000 or more (excluding ISO/IEC 27001 and ISO 27701 certification).[573]

The American Institute of Certified Public Accountants has developed a cybersecurity compliance framework known as Service Organization Control 2 (''SOC 2''). Cybersecurity audit costs can be divided into SOC 2 Type 1 audits and SOC 2 Type 2 audits. Type 1 audits evaluate the suitability of controls at a specific point in time and can cost between $5,000 and $25,000. Type 2 audits gauge the effectiveness of controls over a more extended

[560] Wolford, *supra* note 551.

[561] Int'l Ass'n of Privacy Pros. & Ernst & Young, *IAPP–EY Annual Privacy Governance Report 2018* (2018), *https://iapp.org/media/pdf/resource_center/IAPP_EY_Governance_Report_2018.pdf* [*https://perma.cc/SA8P-QV3G*]; Int'l Ass'n of Privacy Pros. & Ernst & Young, *IAPP–EY Annual Privacy Governance Report 2019* (2019), *https://iapp.org/media/pdf/resource_center/IAPP_EY_Governance_Report_2019.pdf* [*https://perma.cc/DG8X-3W5G*].

[562] Cisco, *supra* note 556.

[563] Florida TaxWatch, *Who Knows What? An Independent Analysis of the Potential Effects of Consumer Data Privacy Legislation in Florida,* TaxWatch Research Blog (Oct. 11, 2021), *https://floridataxwatch.org/Research/Blog/who-knows-whatanalysis-of-data-privacy-legislation-in-florida* [*https://perma.cc/2TD9-RLBR*].

[564] Rob van der Meulen, *4 Key Trends in the Gartner Hype Cycle for Legal and Compliance Technologies, 2020,* Gartner (Sept. 21, 2020), *https://www.gartner.com/smarterwithgartner/4-key-trends-in-the-gartner-hype-cycle-for-legal-and-compliance-technologies-2020* [*https://perma.cc/2AN5-PDTJ*].

[565] *Data Processing Agreement Cost,* ContractsCounsel, *https://www.contractscounsel.com/b/data-processing-agreement-cost* [*https://perma.cc/PDW6-LFZN*].

[566] Clare Sullivan, *EU GDPR or APEC CBPR? A Comparative Analysis of the Approach of the EU and APEC to Cross Border Data Transfers and Protection of Personal Data in the IoT Era,* 35 Comput. L. & Sec. Rev. 380 (2019), *https://doi.org/10.1016/j.clsr.2019.05.004* [*https://perma.cc/EGH9-D7ER*].

[567] *ISO 27701* vs. *APEC CBPR,* nccgroup (July 20, 2023), *https://www.nccgroup.com/us/iso-27701-vs-apec-cbpr/* [*https://perma.cc/8VVW-FYMB*].

[568] Asia-Pac. Econ. Coop., *APEC Privacy Framework* ¶ 32 (2015), *https://www.apec.org/docs/default-source/Publications/2017/8/APEC-Privacy-Framework-(2015)/217_ECSG_2015-APEC-Privacy-Framework.pdf* [*https://perma.cc/C8RN-V2ND*].

[569] Cisco, *supra* note 556, at 9.

[570] *CCPA Assessment Cost,* TrustNet, *https://trustnetinc.com/california-consumer-privacy-act-cost/* [*https://perma.cc/V88J-WW5M*].

[571] *GDPR Certification Cost: Factors, Examples and Benefits,* Neumetric (May 15, 2023), *https://www.neumetric.com/gdpr-certification-cost/* [*https://perma.cc/X8ZM-HW32*].

[572] *Id.*

[573] Ayush Saxena, *Compliance Q&A: How Much Does GDPR Compliance Cost?,* Sprinto (Apr. 3, 2024), *https://sprinto.com/blog/gdpr-compliance-cost/* [*https://perma.cc/NA35-YAQP*].

timeframe and can range in costs from $30,000 to $100,000.[574] The latter is more appropriate for firms processing highly sensitive personal data on a regular basis.[575] ''Dunkelberger provides a slightly different range for SOC 2 Type 1 audits, estimating that they can cost $15,000 to $50,000 for small to medium-sized businesses and between $50,000 to $100,000 for large businesses; and for SOC 2 Type 2 Audits, estimating that they can cost $30,000 to $75,000 for small to medium-sized businesses and $75,000 to $150,000 for large businesses. These costs include the price of a readiness assessment, audit, remediation, and consultant fees.[576]

As these estimates show, the costs of annual audits for compliance with CCPA, GDPR, and SOC 2 range from $3,000 to $150,000, depending on audit type and firm size. The Department expects that such examiners may not always charge these full rates separately just to certify compliance with the proposed rule, due to redundancies with existing legislation and efficiencies of conducting simultaneous audits pursuant to multiple rules. Nevertheless, there would be increased costs, as there are likely to be variations in addition to the redundancies. For purposes of this analysis, the Department assumes that for all small firms, the proposed rule would result in audit costs that are 10 percent of the estimated cost of an audit from the reviewed literature, or $300 ($3,000 * 10 percent incremental cost). The Department assumes that for all large firms, the proposed rule would result in audit costs that are 5 percent of the estimated cost of an audit from the reviewed literature, or $7,500 ($150,000 * 5 percent incremental cost).

v. Estimated Recordkeeping Costs From the Reviewed Literature

The wide-ranging estimates of recordkeeping costs in the studies reviewed, and the entwinement of the former with other costs, demonstrate the difficulty in determining specific costs for each due to the proposed rule. Further, the literature is not specific to compliance with this proposed rule. Rather, the literature relates to the business costs of protecting personal information from unauthorized dissemination while establishing procedures for its processing and transfer, in addition to protocols for responding to consumer preferences regarding handling of their own personal information. In recent years, privacy and protection laws affecting the entities that will likely be impacted by the proposed rule have proliferated. Thus, the recordkeeping costs contemplated under the proposed rule have already been incurred to some extent.

vi. Summary of a Compliance Program: Due Diligence, Recordkeeping, and Auditing

From this examination of the available literature, the due diligence, recordkeeping, and auditing requirements are likely to unevenly impact firms that must comply with the proposed rule, depending on the size of each firm and how much it currently spends on the components of due diligence. Although the means by which firms will comply is uncertain, the Department has relied on a variety of research in the topic areas to make preliminary estimates of costs due to the proposed rule.

Uncertainty is prevalent in these restricted transactions and data-brokerage market cost estimates for several reasons. In particular, the estimates of recordkeeping costs based on the percentage of the costs of compliance with GDPR and other data protection regimes reported in various studies are highly speculative. Estimates of the proposed rule-imposed incremental costs above and beyond similar compliance activities already taking place are also speculative. Consequently, the Department welcomes comments on these cost calculations from affected industries and stakeholders to better inform decision making relative to the proposed rule.

Beyond the cost impacts of the proposed regulation, there could possibly be adjustments and market movements in reaction to changes in the threshold levels that are being proposed. This analysis assumes that all the current bulk U.S. sensitive personal data transactions are above the lower threshold levels as defined by the proposed rule. If the threshold levels are set at the higher level in the final rule, it is possible that there may be less immediate market disruption but also a greater risk of more data falling into malicious hands, including through evasion techniques such as structuring and smurfing (*i.e.,* conducting smaller and more frequent transactions using additional individuals). Since there is no available data on the number of transactions by volume of personal data being transferred, the impacts of selecting one bulk threshold over another within the ranges in the NPRM are uncertain at the time of the proposal, and the Department welcomes comments on this subject.

Note that the recordkeeping costs discussed here (part VII.A of this preamble) are also included in part VII.F of this preamble (Paperwork Reduction Act), which presents cost estimates for the six new information collection requests introduced by the proposed rule. The costs of affirmative annual reporting are also discussed above. In addition to recordkeeping costs and the cost of affirmative annual reporting, part VII.F of this preamble presents estimates for the applications for specific licenses, reports of rejected prohibited transactions, requests for advisory opinions, petitions for removal from the Covered Persons List, and reports of known or suspected violations of onward transfers prohibition. All of those information collections affect a relatively small number of firms. Additional detail on those annual costs is available in the Information Collection Request submitted for Office of Management and Budget review under the Paperwork Reduction Act and publicly available on *reginfo.gov.*

9. Summary of Regulatory Analysis

Regulatory analysis in the areas of national security and foreign policy is often not easily quantifiable or monetizable due to an array of factors, such as inadequate information, inaccessibility of sensitive or proprietary data; and the absence of a good measure of the effectiveness of the regulations.

The purpose of the Preliminary RIA is to gather and analyze enough adequate information to inform agency decision makers about whether a proposed rulemaking is in the public's interest. The analysis should describe the impacts on firms in the market and in the supply chain, remembering that the intermediate firms in the chain are customers of the suppliers. To the extent possible, the impacts on the general public should be considered, as well as—in the case of this proposed rulemaking—the impact on national security and foreign policy and the impact of data-brokerage restrictions on the positive uses of bulk data. The precision of estimates depends on the availability of data, the confidence in the accuracy of the data, and the degree of understanding of the impacted markets.

---

[574] Tim Mektrakarn, *How Much Does a SOC2 Audit Cost in 2024?,* Bright Defense (Aug. 7, 2024), *https://www.brightdefense.com/resources/soc-2-audit-costs/* [*https://perma.cc/G7FD-28Y6*].

[575] Meeba Gracy, *SOC 2 Type 1 vs Type 2 (A Detailed Comparison),* Sprinto (Mar. 16, 2024), *https://sprinto.com/blog/soc-2-type-1-vs-type-2/* [*https://perma.cc/BZL4-GJY4*].

[576] David Dunkelberger, *SOC 2 Budgeting: How Much Does a SOC 2 Audit Cost?,* I.S. Partners: Blog (Nov. 6, 2023), *https://www.ispartnersllc.com/blog/soc-2-audit-cost/* [*https://perma.cc/KCJ8-SMNA*].

These economic impact estimates lack precision due to significant gaps in the available data on the number of firms and data transactions that would be affected by the proposed rule and by the lack of confidence in much of the available data. Due to relatively recent and emerging developments in studying the market for data, relevant, reliable, and representative size, sales, employment, and other descriptive information on the data-brokerage market and other entities that will be subject to the proposed rule does not appear to be currently available. The Department is not aware of reliable data on the exact number of firms that currently engage in prohibited data-brokerage transactions, the size distribution of these firms, or the numbers of firms that sell above or below the threshold levels that would bring them under the proposed rule's umbrella. The Department welcomes additional input on this point. The low and high threshold levels for the different categories of sensitive personal data or government-related data vary by factors of 10 to 1 for human genomic data and 1,000 to 1 for personal health data and personal financial data. Furthermore, the Department lacks data on the broader universe of firms that transact in government-related data or bulk U.S. sensitive personal data in the context of restricted transactions. As noted in the NPRM, firms that transact in bulk U.S. sensitive personal data above the proposed thresholds, as laid out in part V.C of this preamble, will need to ensure that their typical data transfers are not in fact going to countries of concern or covered persons (for prohibited transactions) and to comply with the security and due diligence requirements for restricted transactions.

This analysis leverages the limited available data on the number of data-brokerage firms and the volume of data-brokerage exports, along with estimates of security and due diligence costs from studies of similar policies and guidelines. The Department finds that, based on certain assumptions, the proposed rule will have at least some measurable economic impacts. From Table VII–10 of this preamble, the Department estimates that the total annual value of lost transactions is $361 million, or an estimated $80,222 per firm for 4,500 firms (3,000 data brokers + 1,500 firms engaged in restricted transactions).

Table VII–14 of this preamble presents estimates of security compliance costs derived from data shown in part VII.B.2 of this preamble and estimates of due diligence, recordkeeping, and auditing costs derived from data shown in part VII.A.8.c of this preamble. The variations in costs are due to firm size and other factors. As explained in part VII.A.8.c of this preamble, the Department estimates the KYC/KYV (*i.e.,* due diligence) costs for verifying one business and its executives to be between a lower bound of $150 and an upper bound of $4,230. There is no information on how many verifications a firm will do, but the Department assumes for purposes of this analysis 10 verifications per firm per year, for a total cost of between $1,500 and $42,300. Adding the lower bounds of due diligence costs ($1,500), auditing costs ($300), and recordkeeping costs ($960) per firm, the resulting costs at a lower bound are $2,760 per firm for other compliance costs. Adding the upper bound of due diligence costs ($42,300), audit costs ($7,500), and recordkeeping costs ($225,000) per firm, the resulting costs are $274,800 for total compliance annual costs per large firm. Table VII–14 of this preamble shows annual compliance costs per firm. The Department welcomes additional input on this point.

TABLE VII–14—ANNUAL COMPLIANCE COSTS PER FIRM

[For Firms Engaged in Restricted Transactions]

Cost category	Low (small firms)	High (large firms)
Security: One-Time Costs	$60,000	$245.000
Security: Recurring Costs	23,620	101,160
Other Compliance Costs (Due Diligence, Audits, Recordkeeping)	2,760	274,800

When the proposed rule is finalized and becomes effective, market dynamics will set in, and firms will exit and enter the market as they adjust to the new regulatory environment. As noted in part VII.A.3.b of this preamble, the U.S. data-brokerage market ranges from around $30 billion to $180 billion per year, suggesting average revenues per firm at around $10 million to $60 million per year, assuming an estimated 3,000 firms. The compliance costs per firm will determine whether firms pursue restricted transactions.

For the purposes of this estimate, the Department assumes that 1,500 firms will engage in restricted transactions, the largest 100 will incur the high costs, and the remaining 1,400 will incur the lower costs. Although it is estimated that there are a relatively few U.S.-based firms conducting business with Chinese cloud-service providers that may continue these activities under the restrictions, it is expected that a large—but unknown—number of other firms will pursue the restricted transaction opportunities involving employment and investment agreements. Under these conditions, the Department assumes that about 1,500 firms beyond the 3,000 data brokers will be active in pursuing vendor, employment, and investment agreement opportunities in the restricted transactions market, the 100 largest of which will be at the high cost and 1,400 of which will incur the lower costs.

The annualized costs of the proposed rule are determined by deriving the 10-year projections for three cost components: the economic value of lost transactions, security costs, and other compliance costs (due diligence, auditing, and recordkeeping). Our analysis assumes that 4,500 firms, including 3,000 data brokers and 1,500 other firms engaged in restricted transactions, will incur economic costs. The analyses also assume that 4,300 of those firms are small firms (including 2,900 data brokers and 1,400 firms engaged in restricted transactions) and 200 of those firms are large firms (100 data brokers and 100 firms engaged in restricted transactions). The analysis also assumes that the data-brokerage industry affected by the proposed rule is growing at a 5-percent annual rate.

Turning to compliance costs, our analyses assume that 1,500 firms will incur compliance costs as a result of the proposed rule. The Department assumes that security costs have one-time components—initial assessment and remediation—that are only realized in the first year, as well as recurring components—ongoing remediation, compliance audits, and training—that

are present for all 10 years. In addition, it is assumed that the other compliance costs, including affirmative due diligence, auditing, and recordkeeping costs, will decline as firms become more efficient and learn to pursue lower-cost compliance options. These due diligence, auditing, and recordkeeping costs are presented as annually decreasing, but at a decreasing rate. As companies move away from reliance on employees in countries of concern or vendors in countries of concern, the Department assumes that these costs will decrease over time. Further, since the security measures are all reliant on existing NIST standards and CISA performance goals to which many companies already align their security posture, the Department assumes that due diligence, auditing, and recordkeeping costs will decrease 15 percent in the second year, 12 percent in the third year, 9 percent in the fourth year, 7 percent in the fifth year, and then 5 percent, 4 percent, 3 percent, 2 percent, and 1 percent in each of the sixth through tenth years. The costs are presented undiscounted (0-percent rate) and at discounted by 2 percent.

In sum, the parameter assumptions of the 10-year projections are:

1. The annual growth rate of the economic value of lost transactions is 5 percent, compounded annually.

2. Due diligence, auditing, and recordkeeping costs in Year 1 are taken from Table VII–14 of this preamble. Costs in Years 2 through 10 decrease, but at a decreasing rate of 15 percent, 12 percent, 9 percent, 7 percent, 5 percent, 4 percent, 3 percent, 2 percent, and 1 percent.

3. Security costs have both one-time and recurring components in Year 1 and only recurring components in Years 2 through 10 (as shown in Table VII–14 of this preamble).

4. The analysis assumes either undiscounted costs or a 2-percent annual discount rate.

5. The value of lost transactions is from Table VII–10 of this preamble.

6. Small firms will bear ''low'' costs shown in the security cost and lost transaction totals, and large firms will bear the ''high'' costs shown in the security cost and lost transaction totals in Tables VII–15 and VII–16 of this preamble.

7. One thousand five hundred (1,500) firms will incur compliance costs as a result of the proposed rule, and a broader group of 4,500 firms will incur costs due to lost transactions.

The 10-year annualized cost analysis (undiscounted and for a 2-percent discount rate) for security and other compliance costs (due diligence, auditing, and recordkeeping costs) is presented in Table VII–15 of this preamble for the 1,400 small firms and in Table VII–16 of this preamble for the 100 large firms. These estimates for security, due diligence, auditing, and recordkeeping costs for both small and large firms engaged in restricted transactions are combined with the industry-wide estimates for the economic value of lost transactions to obtain total costs for all firms, which are presented in Table VII–17 of this preamble.

TABLE VII–15—10-YEAR ANNUALIZED COST ANALYSIS FOR SECURITY, DUE DILIGENCE, AUDITING (AND RECORDKEEPING) FOR (THE 1,400) SMALL FIRMS

[Millions of dollars]

Cost category	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10	Total	Annualized
Undiscounted												
Security	$117	$35	$36	$38	$40	$42	$44	$47	$49	$51	$500	$50
Due Diligence, Audits, and Recordkeeping	4	3	3	3	3	3	3	3	3	3	33	3.3
Total	121	38	40	41	43	45	47	50	52	55	532	53
Discount Rate: 2 Percent												
Security	117	34	35	36	37	38	39	41	42	43	463	46
Due Diligence, Audits, and Recordkeeping	4	3	3	3	3	3	3	3	3	3	30	3.0
Total	121	37	38	39	40	41	42	43	45	46	493	49

Key Assumptions: Industry growth rate of 5 percent; due diligence, auditing, and recordkeeping costs decreasing at a decreasing rate of 15–12–9–7–5–4–3–2–1 percent over years 2–10.

These year-to-year changes are the same in percentage terms for the analysis of large firms in Table VII–16 of this preamble.

TABLE VII–16—10-YEAR ANNUALIZED COST ANALYSIS FOR SECURITY AND DUE DILIGENCE (AND RECORDKEEPING) FOR (THE 100) LARGE FIRMS

[Millions of dollars]

Cost category	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10	Total	Annualized
Undiscounted												
Security	$35	$11	$11	$12	$12	$13	$14	$14	$15	$16	$152	$15
Due Diligence, Audits, and Recordkeeping	27	25	23	22	22	22	22	22	23	24	232	23

TABLE VII–16—10-YEAR ANNUALIZED COST ANALYSIS FOR SECURITY AND DUE DILIGENCE (AND RECORDKEEPING) FOR (THE 100) LARGE FIRMS—Continued

[Millions of dollars]

Cost category	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10	Total	Annualized
Total	62	35	34	34	34	35	35	37	38	40	383	38
Discount Rate: 2 Percent												
Security	35	10	11	11	11	12	12	12	13	13	140	14
Due Diligence, Audits, and Recordkeeping	27	24	22	21	20	19	19	19	19	20	212	21
Total	62	35	33	32	31	31	31	32	32	33	352	35

Key Assumptions: Industry growth rate of 5 percent; due diligence, auditing, and recordkeeping costs decreasing at a decreasing rate of 15–12–9–7–5–4–3–2–1 percent over years 2–10.

The total annualized costs of the proposed rule for small and large firms are combined and presented in Table VII–17 of this preamble, estimated at $549 million undiscounted and $502 million discounted at 2 percent (any differences are due to rounding). Tables VII–15 and VII–16 of this preamble only include the costs of the security, due diligence, and recordkeeping requirements of the proposed rule, while Table VII–17 of this preamble also includes the costs associated with the value of lost transactions.

TABLE VII–17—10-YEAR ANNUALIZED COST ANALYSIS FOR ALL FIRMS

[Millions of dollars]

Cost category	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10	Total	Annualized
Undiscounted												
Lost Transactions	$364	$382	$401	$421	$442	$465	$488	$512	$538	$565	$4,578	$458
Security	152	45	48	50	52	55	58	61	64	67	652	65
Due Diligence, Audits, and Recordkeeping	31	28	26	25	25	25	25	25	26	27	264	26
Total	547	456	475	497	520	544	571	598	628	659	5,494	549
Discount Rate: 2 Percent												
Lost Transactions	364	375	22	398	410	422	435	448	461	475	4,173	417
Security	152	44	46	47	49	50	52	53	55	56	604	60
Due Diligence, Audits, and Recordkeeping	31	28	25	24	23	22	22	22	22	23	241	24
Total	547	447	93	469	481	494	508	523	538	554	5,018	502

Key Assumptions: Industry growth rate of 5 percent; due diligence, auditing, and recordkeeping costs decreasing at a decreasing rate of 15–12–9–7–5–4–3–2–1 percent over years 2–10.

Table VII–18 of this preamble summarizes the 10-year annualized cost analysis (presented in Tables VII–15, VII–16, and VII–17 of this preamble) for small and large firms separately and in total, both undiscounted and with a discount rate of 2 percent.

This cost estimate reflects the likelihood that a number of smaller firms will drop out of the market if the costs of compliance are greater than expected revenues (*i.e.,* if marginal costs exceed marginal revenues). Of course, this could also be true of larger firms that lack the infrastructure or financial resources to comply with the proposed rules and therefore choose to forgo certain transactions or business operations in that market altogether.

In addition to the potential decrease in the number of firms in the industry, another related effect is that the proposed rule may create a barrier to entry for potential data brokers. That is, the same compliance burdens that affect marginal current brokers will also affect potential ones.

TABLE VII–18—SUMMARY OF TOTAL 10-YEAR ANNUALIZED COSTS

[Undiscounted and for a 2-Percent Discount Rate]

Discount rate	Total cost
Undiscounted	$549,000,000
2 Percent	502,000,000

These preliminary estimated costs of the proposed rule appear to be reasonable when balanced against the expected benefits of preventing the potential risk and harms to national security and foreign policy that are possible when government-related data or bulk U.S. sensitive personal data is transferred to foreign adversaries. These

benefits are beyond monetary calculation but suggest that the proposed rule will have very large net benefits, including protections to well over 100 million American individuals who are potential targets of adversaries using government-related data or bulk U.S. sensitive personal data. A wide range of benefits of the regulation will also be realized by firms, including the savings associated with potentially reducing the likelihood of data breaches thanks to improved security, which are estimated to cost an average of $4.88 million per breach.[577] And firms that sell data to, or buy data from, brokers will have increased confidence in the security and due diligence arrangements associated with the regulation.

Both the benefits to be realized and the costs to the economy and government will be determined, to some extent, by the effectiveness of compliance and enforcement activities and by the methods that market participants use to attempt to avoid detection of prohibited or restricted activities. For example, ''back doors'' are used to circumvent economic sanctions, and digital assets are used to hide sanctioned transactions themselves. The countries of concern are known to conduct commercial and military operations through proxies. As shown in parts IV.D.1.b and IV.D.1.f of this preamble, Cuba and Venezuela have acted as third parties to promote malicious acts by other countries of concern. Unless the due diligence requirements are fully complied with and the due diligence procedures and inquiries provide accurate information, the effectiveness of the proposed rule may be weakened, leading to reduced expected benefits.

One commenter suggested that the Department conduct a retrospective review of the impact after the final rule becomes effective. The Order already requires such a review. Under section 5 of the Order, within 1 year after the final rule becomes effective, the Department must submit a report to the President that addresses, to the extent practicable, the effectiveness of the measures imposed under the Order in addressing threats to the national security of the United States described in the Order and the economic impact of the implementation of the Order, including on the international competitiveness of U.S. industry. The Order requires the Department to solicit public comment in evaluating the economic impact. The Department also intends to regularly monitor the effectiveness and impact of the regulations once they become effective.

TABLE VII–19—OMB CIRCULAR A–4 ACCOUNTING STATEMENT PROVISIONS PERTAINING TO PREVENTING ACCESS TO U.S. SENSITIVE PERSONAL DATA AND GOVERNMENT-RELATED DATA BY COUNTRIES OF CONCERN OR COVERED PERSONS NPRM

Category	Estimate			Units			Notes
	Primary	Low	High	Dollar year	Discount rate	Time horizon	
Benefits							
Annualized monetized benefits	The benefits of the proposal include the security of the American people, economic prosperity and opportunity, and democratic values, all of which are beyond a reasonable, reliable, and acceptable estimate of quantified monetary value. Details in NPRM.						
Annualized quantified, but non-monetized, benefits.	The Department did not identify any benefits that were quantified.						
Unquantified benefits	Discussed in NPRM.						
Cost							
Annualized monetized costs	$549,000,000	.....	.....	.....	undiscounted	Years 1–10	The primary costs of the proposed rule are the lost value of transactions due to the prohibitions and costs related to the restrictions that will require due diligence expenditures for enhanced security, KYC/KYV verifications, recordkeeping, reporting, and audits.
	$502,000,000	.....	.....	.....	2%	Years 1–10	
Annualized quantified, but non-monetized, costs.	.....	.....	.....	.....	.....	.....	
Unquantified costs	.....	.....	.....	.....	.....	.....	
Transfers							
Annualized monetized Federal budgetary transfers. *From/To:*.	.....	.....	.....	.....	.....	.....	
Other annualized monetized transfers *From/To:*.	.....	.....	.....	.....	.....	.....	
Effects							
Effects on State, local, or Tribal governments.	The proposed rule would not have Tribal implications warranting the application of Executive Order 13175. It would not have substantial direct effects on one or more Indian Tribes, on the relationship between the Federal Government and Indian Tribes, or on the distribution of power and responsibilities between the Federal Government and Indian Tribes.						
Effects on small businesses	This analysis assumes that the small entities affected by the proposed rule will incur compliance costs of around $32,380 per firm annually, compared with an annual compliance cost of $400,460 for the largest affected firms. Both cost figures are undiscounted. The Department estimates that the proposed rule will impact just over 4,000 small entities, and that the highest-cost scenario will apply to approximately 100 firms.						
Effects on wages	The Department did not estimate any impacts on wages.						

[577] *Cost of a Data Breach Report 2024,* IBM, *https://www.ibm.com/reports/data-breach* [*https://perma.cc/8GNL-YEUX*].

TABLE VII–19—OMB CIRCULAR A–4 ACCOUNTING STATEMENT PROVISIONS PERTAINING TO PREVENTING ACCESS TO U.S. SENSITIVE PERSONAL DATA AND GOVERNMENT-RELATED DATA BY COUNTRIES OF CONCERN OR COVERED PERSONS NPRM—Continued

Category	Estimate			Units			Notes
	Primary	Low	High	Dollar year	Discount rate	Time horizon	
Effects on growth	The Department did not estimate any impacts on growth.						

B. Regulatory Flexibility Act

The Department is proposing this rule to address the growing threat posed by the efforts of foreign adversaries to access and exploit the government-related data or Americans' bulk U.S. sensitive personal data. On February 28, 2024, the President issued Executive Order 14117 on ''Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern.'' This Order directs the Attorney General to, among other things, determine which classes of data transactions ought to be prohibited due to the unacceptable risk they pose by allowing countries of concern or covered persons to access government-related data or bulk U.S. sensitive personal data. The Order also directs the Attorney General to work with relevant agencies to identify countries of concern and classes of covered persons, establish a process to issue licenses authorizing transactions that would otherwise be prohibited or restricted transactions, address the need for requirements for recordkeeping and reporting transactions, and determine which classes of transactions will be required to comply with separate security requirements.

The need for the proposed rule stems from the increased efforts that countries of concern are making to obtain sensitive personal data of Americans and to utilize it in a way that undermines national security and foreign policy. Advances in computing technology, artificial intelligence, and methods for processing large datasets allow countries of concern to more effectively leverage collected data for malicious purposes. The capability currently exists to allow those who government-related data or Americans' bulk U.S. sensitive personal data to combine and manipulate it in ways that could identify sensitive personal data, including personal identifiers and precise geolocation information.

1. Succinct Statement of the Objectives of, and Legal Basis for, the Proposed Rule

Through the Order, the President used his authority under IEEPA and the National Emergencies Act to declare national emergencies and regulate certain types of economic transactions in order to protect the country against foreign threats. The Order expands upon the national emergency previously declared by Executive Order 13873 of May 15, 2019 (Securing the Information and Communications Technology and Services Supply Chain), which was modified by Executive Order 14034 of June 9, 2021 (Protecting Americans' Sensitive Data from Foreign Adversaries). Furthermore, the President, under title 3, section 301 of the U.S. Code, authorized the Attorney General, in consultation with the heads of relevant executive agencies, to employ the President's powers granted by IEEPA as may be necessary or appropriate to carry out the purposes of the Order.

IEEPA empowers the President to ''investigate, regulate, or prohibit'' foreign exchanges in cases where there is a threat coming from outside the United States that threatens the country's ''national security, foreign policy, or economy.'' Existing IEEPA-based programs include those administered by OFAC, which enforces economic and trade sanctions, and the Department of Commerce's Bureau of Industry and Security, which is responsible for information and communications technology and services supply chain security.

2. Description of and, Where Feasible, an Estimate of the Number of Small Entities to Which the Proposed Rule Will Apply

The proposed rule would affect data-brokerage firms and other firms engaged in covered data transactions that pose a risk of exposing government-related data or bulk U.S. sensitive personal data to countries of concern or covered persons. The Department has estimated that about 4,500 firms, just over 90 percent of which are small businesses (hereafter referred to as ''small entities''), would be impacted by the proposed rule. Therefore, the Department estimates that this proposed rule would impact approximately 4,050 small entities and approximately 450 firms that would not be classified as small entities.

Small entities, as defined by the Regulatory Flexibility Act, include small businesses, small nonprofit organizations, and small governmental jurisdictions. The definition of ''small entities'' includes the definition of ''small businesses'' pursuant to section 3 of the Small Business Act of 1953, as amended: ''A small business concern . . . shall be deemed to be one which is independently owned and operated, and which is not dominant in its field of operation.'' The definition of ''small business'' varies from industry to industry (as specified by NAICS code and found in 13 CFR 121.201) to reflect the typical company size in each industry.

NAICS code 518210, ''Computing Infrastructure Providers, Data Processing, Web Hosting, and Related Services,'' contains all the affected data brokers as well as some of the other entities engaged in one or more of the classes of restricted data transactions.[578] The number of small entities affected by the proposed rule was estimated by using the Small Business Administration (''SBA'') small business size standard for the NAICS code to calculate the proportion of firms that are considered small entities. Data brokers are only a subset of the total firms contained in the identified NAICS code; however, for this analysis, it was assumed that the proportion of small entities was the same for both the broader NAICS industry and the specific data broker industry. Because more than 90 percent of impacted firms across all relevant industries can be considered small entities, the proposed rule would have an impact on a substantial number of small entities.

[578] *518210—Computing Infrastructure Providers, Data Processing, Web Hosting, and Related Services,* North American Industry Classification System, *https://www.naics.com/naics-code-description/?v=2022&code=518210* [*https://perma.cc/5PWG-AQWL*].

TABLE VII–20—SMALL BUSINESS SIZE STANDARD AND AFFECTED FIRMS

Number of affected firms	Share of affected firms that are small	Number of affected small firms
4,500	Approximately 90 percent	Approximately 4,050.

This analysis assumes that the small entities affected by the proposed rule will incur compliance costs of around $32,380 per firm per year, compared with an annual compliance cost of $400,460 for the largest affected firms.

The Department is not aware of reliable revenue data by firm size for the data broker industry, but a reasonable assumption is that if a firm's revenues from data sales are not sufficient to cover the compliance costs, then that firm will have an incentive to exit that market. Furthermore, calculating the proportion of the costs associated with the proposed rule that falls on small firms is complicated by the fact that several of the proposed rule's provisions—specifically the requirements related to cybersecurity, due diligence, recordkeeping, and reporting—likely involve high fixed costs. Even if small entities have less complex business operations, leading to fewer complications related to compliance, they may still face a higher cost burden from the proposed rule than larger firms. Large entities will likely already have a greater portion of the fixed costs associated with the proposed rule covered by existing capabilities. Therefore, while the costs associated with the security and due diligence requirements will be smaller in absolute terms for smaller entities, such entities will likely need to pay a higher proportion of their overall budgets to comply. Due to the unknowns and the large number of small entities, it is possible that a substantial number of small firms will experience a significant impact. The Department welcomes comments on this topic.

3. Description of the Projected Reporting, Recordkeeping, and Other Compliance Requirements of the Proposed Rule

The proposed rule would require firms engaged in restricted transactions to adhere to certain standards for data security, due diligence, recordkeeping, and reporting. *See* § 202.401. To mitigate the risk of sharing government-related data or bulk U.S. sensitive personal data with countries of concern or covered persons through restricted transactions, organizations engaged in restricted transactions would be required to institute organizational and system-level cybersecurity policies, practices, and requirements and data-level requirements developed by DHS through CISA in coordination with the Department. *See* § 202.402. Those requirements, which CISA will release through a separate Request For Information, overlap with several similar, widely used cybersecurity standards or frameworks. In addition, the security requirements developed by CISA would require firms to protect the data associated with restricted transactions using combinations of the following capabilities necessary to prevent access to covered data by covered persons or countries of concern:

1. data minimization and data masking;
2. encryption;
3. privacy-enhancing technologies; and
4. denial of access.

Firms will also be required to undergo annual independent testing and auditing to ensure their continuing compliance with the security requirements.

Additionally, in order to ensure that government-related data or Americans' bulk U.S. sensitive personal data are not accessible by countries of concern or covered persons, firms will be required to engage in due diligence before pursuing restricted transactions, which involves utilizing KYC/KYV programs to complete background checks on potential partners. Furthermore, firms will be required to keep records that contain extensive details of their restricted transactions as well as the details of the other parties involved. They will also be required to undergo annual audits of their records to ensure compliance and assess potential risks.

4. Identification of All Relevant Federal Rules That May Duplicate, Overlap, or Conflict With the Proposed Rule

As discussed in part IV.K of this preamble, while the PADFAA seeks to address some of the same national security risks of the proposed rule, there are clear differences between the PADFAA, the Order, and this proposed rule, including the scope of regulated data brokerage activities, the types of bulk sensitive personal data that are covered, and the relevant countries of concern. Further, while the PADFAA allows the FTC to investigate certain data-brokerage activities involving countries of concern as unfair trade practices consistent with the FTC's existing jurisdiction, the proposed rule establishes a new set of consistent regulatory requirements that apply across multiple types of commercial transactions and sectors. Finally, as stated in part IV.K of this preamble, the Department will coordinate closely with the FTC to ensure consistency in how both authorities are implemented.

Some restricted transactions under the proposed rule could also end up being subject to review and action by CFIUS. The Foreign Investment Risk Review Modernization Act of 2018 gave CFIUS the authority to review certain non-controlling foreign investments that may pose a risk to national security by allowing the sensitive personal data of U.S. citizens to be exploited.[579] However, while CFIUS acts on a transaction-by-transaction basis, the proposed rule would create restrictions and prohibitions on covered data transactions that would apply to categories of data transactions involving the six countries of concern. In a situation where a covered data transaction regulated by the proposed rule was later subject to a CFIUS review, it would be exempt from the proposed rule to the extent that CFIUS takes any of the actions identified in the proposed rule. *See* §§ 202.207; 202.508.

Furthermore, the categories of covered data transactions covered by the proposed rule extend beyond the scope of CFIUS, including the provision of government-related data or bulk U.S. sensitive personal data through data brokerage, vendor agreements, and employment agreements. The proposed rule also covers investment agreements that may not be covered by CFIUS as well as cases where the relevant risks do not result from the covered transaction or may occur before a CFIUS action takes place.

C. Executive Order 13132 (Federalism)

The proposed rule would not have federalism implications warranting the application of Executive Order 13132. The proposed rule does not have substantial direct effects on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government.

[579] *See* Foreign Investment Risk Review Modernization Act of 2018, supra note 11.

D. Executive Order 13175 (Consultation and Coordination With Indian Tribal Governments)

The proposed rule would not have Tribal implications warranting the application of Executive Order 13175. It does not have substantial direct effects on one or more Indian Tribes, on the relationship between the Federal Government and Indian Tribes, or on the distribution of power and responsibilities between the Federal Government and Indian Tribes.

E. Executive Order 12988 (Civil Justice Reform)

This proposed rule meets the applicable standards set forth in sections 3(a) and 3(b)(2) of Executive Order 12988.

F. Paperwork Reduction Act

The collections of information contained in this notice of proposed rulemaking have been submitted to the Office of Management and Budget for review in accordance with the Paperwork Reduction Act of 1995, 44 U.S.C. 3507(d), under control number 1124–AA01.

Written comments on this collection can be submitted by visiting *www.reginfo.gov/public/do/PRAMain.* Find this document by selecting ''Currently Under Review—Open for Public Comments'' or by using the search function. Comments on the collection of information should be received by November 29, 2024.

The Department of Justice is soliciting comments from members of the public concerning this collection of information to:

- Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;
- Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information;
- Enhance the quality, utility, and clarity of the information to be collected; and
- Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated collection techniques or other forms of information technology.

The proposed rule includes seven new collections of information: annual reports; applications for specific licenses; reports on rejected prohibited transactions; requests for advisory opinions; petitions for removal from the designated Covered Persons List; reports of known or suspected violations of the onward transfers prohibition; and recordkeeping requirements for restricted transactions.

Based on wage rates from the Bureau of Labor Statistics and lower- and upper-bound estimates (used because this is a new program and there is uncertainty in the estimated number of potential respondents for each of the forms), the following are the estimated burdens of the proposed collections:

- *Annual reports.* The Department estimates that 375 to 750 filers will send an average of one annual report per year, spending an estimated average of 40 hours to prepare and submit each annual report. The Department estimates the aggregated costs for all filers at $821,100 to $1,642,200 annually for annual reports.
- *Applications for specific licenses.* The Department estimates that 15 to 25 filers will send an average of one application for a specific license per year, spending an estimated average of 10 hours to prepare and submit each application for a specific license. The Department estimates the aggregated costs for all filers at $8,211 to $13,685 annually for applications for specific licenses.
- *Reports on rejected prohibited transactions.* The Department estimates that 15 to 25 filers will send an average of one report on a rejected prohibited transaction per year, spending an estimated average of 2 hours to prepare and submit each application for a specific license. The Department estimates the aggregated costs for all filers at $1,642 to $2,737 annually for reports on rejected prohibited transactions.
- *Requests for advisory opinions.* The Department estimates that 50 to 100 filers will send an average of one request for an advisory opinion per year, spending an estimated average of 2 hours to prepare and submit each request for an advisory opinion. The Department estimates the aggregated costs for all filers at $5,474 to $10,948 annually for requests for advisory opinions.
- *Petitions for removal from covered persons list.* The Department estimates that 15 to 25 filers will send an average of one petition for removal from the Covered Persons List per year, spending an estimated average of 5 hours to prepare and submit each petition for removal from the Covered Persons List. The Department estimates the aggregated costs for all filers at $4,106 to $6,843 annually for petitions for removal from the Covered Persons List.
- *Reports of known or suspected violations of onward transfers prohibition.* The Department estimates that 300 to 450 filers will send an average of one report of known or suspected violations of the onward transfers prohibition per year, spending an estimated average of 2 hours to prepare and submit each report of known or suspected violations of the onward transfers prohibition. The Department estimates the aggregated costs for all filers at $32,844 to $49,266 annually for reports of known or suspected violations of the onward transfers prohibition.
- *Recordkeeping requirements for restricted transactions.* The Department estimates that 1,400 small to medium-sized firms will incur a total of $1,344,000 in recordkeeping costs per year. Also, the Department estimates that 100 large firms will incur a total of $84,844,000 in recordkeeping costs per year.

Under the Paperwork Reduction Act, an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid control number assigned by the Office of Management and Budget.

G. Unfunded Mandates Reform Act

The Unfunded Mandates Reform Act requires that Federal agencies prepare a written statement assessing the effects of any Federal mandate in a proposed or final agency rule that may directly result in the expenditure of $100 million or more in 1995 dollars (adjusted annually for inflation) in any 1 year by State, local, and Tribal governments, in the aggregate, or by the private sector (2 U.S.C. 1532(a)). However, the Unfunded Mandates Reform Act does not apply to ''any provision'' in a proposed or final rule that is ''necessary for the national security'' (2 U.S.C. 1503(5)).

In the Order, the President explained that ''[t]he continuing effort of certain countries of concern to access Americans' sensitive personal data and United States Government-related data constitutes an unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security and foreign policy of the United States.'' The Order expanded the scope of 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). Section 2(a) of the Order thus requires the Attorney General to issue the regulations in this

part, subject to public notice and comment, ''[t]o assist in addressing the national security emergency described'' in the Order. Because the entirety of this proposed rule and every provision in it addresses the national emergency described by the President in the Order, the Department has concluded that the Unfunded Mandates Reform Act does not apply to this proposed rule.

List of Subjects in 28 CFR Part 202

Computer technology, Health records, Incorporation by reference, Investments, Military personnel, National security, Personally identifiable information, Privacy, Reporting and recordkeeping requirements, Security measures.

■ Under the rulemaking authority vested in the Attorney General in 5 U.S.C. 301; 28 U.S.C. 509, 510 and delegated to the Assistant Attorney General for National Security by A.G. Order No. 6067–2024, and for the reasons set forth in the preamble, the Department of Justice proposes to add part 202 to chapter I of title 28 of the Code of Federal Regulations to read as follows:

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

Sec.

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

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 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 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.

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

(a) Human genomic data collected about or maintained on 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 (g) 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 bulk data relating to U.S. persons, in any format, regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted.

§ 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 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, (1) 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 (2) 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 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) [Reserved]

§ 202.211 Covered person.

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

(1) A foreign person that is an entity that is 50 percent or more owned, directly or indirectly, by a country of concern, 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 percent or more owned, directly or indirectly, by an entity described in paragraph (a)(1) of this section or a person described in paragraphs (a)(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 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 person that is an entity and the employee is a foreign person, the person is a covered person.

§ 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.

(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 covered 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 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 the bulk precise geolocation data, IP address, and advertising IDs of its U.S. users' devices to an advertising exchange based in a country of concern. The U.S. company's provision of this data as part of the sale of advertising space is data brokerage and a prohibited 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.

§ 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 the applicable prohibitions and directives contained in this part, which is 12:01 a.m. ET on [date to be determined].

§ 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 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.

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:

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

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

(c) 3001.90.0115 Glands and other organs, dried, whether or not powdered

(d) 3002.12.0010 Human blood plasma

(e) 3002.12.0020 Normal human blood sera, whether or not freeze-dried

(f) 3002.12.0030 Human immune blood sera

(g) 3002.12.0090 Antisera and other blood fractions, Other

(h) 3002.51.0000 Cell therapy products

(i) 3002.59.0000 Cell cultures, whether or not modified, Other

(j) 3002.90.5210 Whole human blood

(k) 3002.90.5250 Blood, human/animal, other

(l) 9705.21.0000 Human specimens and parts thereof

§ 202.224 Human genomic data.

The term *human genomic data* means 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.

§ 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 nonproliferation 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 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, 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.

(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 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);

(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 relates to the past, present, or future physical or mental health or condition of an individual; the provision 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 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 (incorporated by reference, *see* § 202.402).

§ 202.249 Sensitive personal data.

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

(b) *Exclusions.* The term *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.

§ 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 ''telecommunications service'' as defined in 47 U.S.C. 153(53).

§ 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 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 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 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 a covered data transaction involving 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 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.

§ 202.303 Prohibited human genomic 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 genomic data, or to human biospecimens from which bulk human genomic 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.

(6) *Example 6.* 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. For the purpose of evasion, a U.S. subsidiary of a company headquartered in a country of concern licenses the derivative algorithm from the U.S. online gambling company for the purpose of accessing bulk sensitive personal identifiers from the training data contained in the algorithm 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 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 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. 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 required by subpart D of this part and all other applicable requirements under this part.

(b) This subpart does not apply to covered data transactions involving access to bulk human genomic data or human biospecimens from which such data can be derived that is subject to the prohibition in § 202.303 of this part.

(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, 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.

§ 202.402 Incorporation by reference.

(a) *Incorporation by reference.* Certain material is incorporated by reference into this part 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.* You may also obtain the material from the National Security Division at *https://www.justice.gov/nsd.* For information on the availability of this material at NARA, visit *www.archives.gov/federal-register/cfr/ibr-locations.html* or email *fr.inspection@nara.gov.* The material may also be obtained from the sources in the following paragraphs of this section.

(b) *Other sources.* The Cybersecurity and Infrastructure Security Agency, Mail Stop 0380, Department of Homeland Security, 245 Murray Lane, Washington, DC 20528–0380, *central@cisa.gov,* 888–282–0870, *http://www.cisa.gov.* You may also obtain the material from the Cybersecurity and Infrastructure Security Agency at *https://www.cisa.gov/.*

(1) The Cybersecurity and Infrastructure Agency (''CISA''), Security Requirements for Restricted Transactions; (Final edition 202X Draft), IBR approved for §§ 202.248; 202.304(b)(4); 202.401(a); 202.401(c)(1); 202.401(c)(2); 202.508(b)(8); 202.508(b)(10); 202.508(b)(11); 202.1001(b)(4); 202.1002(b)(1); 202.1002(e)(4); 202.1002(f)(2)(iv); 202.1002(f)(2)(v); 202.1002(f)(2)(vi); 202.1101(b)(2); 202.1101(b)(3).

(2) [Reserved]

Subpart E—Exempt Transactions

§ 202.501 Personal communications.

Subparts C and D of this part do 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.

Subparts C and D of this part do 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.

Subparts C and D of this part do 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 Official business of the United States Government.

(a) *Exemption.* Subparts C and D 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) [Reserved]

§ 202.505 Financial services.

(a) *Exemption.* 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 the

provision of financial services, including:

(1) Banking, capital-markets (including investment-management services), 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 executing trades within a securities 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.

(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.

(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, but it is an exempt transaction that is ordinarily incident to and part of facilitating 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 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 are ordinarily incident to and part of U.S. consumers' purchase of goods.

(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 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 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 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. bank operates a foreign branch in a country of concern and provides financial services to U.S. persons living within the country of concern. The bank 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 sensitive personal data of U.S. persons resident in the country or U.S. persons conducting transactions through the foreign branch. Responding to the regulator's request, including providing access to this bulk 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 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 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 access the bulk personal financial data. The appointment of the director, who is a covered person, is a restricted employment agreement and is not exempt because the board member 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 and D 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.

§ 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 and D 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) 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);

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

(11) 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);

(12) 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);

(13) 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

(14) 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;

(2) The Global Influenza Surveillance and Response System; and

(3) The Agreement between the Government of the United States of America and the Government of the People's Republic of China on Cooperation in Science and Technology (1979).

(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 and D 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 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 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(l)(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 and D 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, including international calling, mobile voice, and data roaming.

(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.* Subparts C and D of this part do not apply to a data transaction that

(1) Involves ''regulatory approval data'' as defined in this section and

(2) Is necessary to obtain or maintain regulatory approval to market a drug, biological product, device, or a combination product in a country of concern, 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 de-identified sensitive personal data that is required to be submitted to a country of concern regulatory entity 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 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 the U.S. company enters a vendor agreement with a covered person located in the country of concern to store, organize, and prepare the bulk U.S. sensitive personal data for submission to the regulatory agency. The transaction is not exempt under this section, because the use of a covered person to prepare the regulatory submission is not necessary to obtain regulatory approval.

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

(a) *Exemption.* Subparts C and D 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 the FDA, provided the data is deidentified.

(b) [Reserved]

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 other agencies as the Attorney General deems appropriate, the Attorney General determines the person meets any of the criteria 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:

(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 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, 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 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 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 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 information 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 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 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 the effective date of this part, 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 of this part 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 engage in any restricted transactions under § 202.401 of this part shall conduct an audit that complies with the requirements of this section.

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

(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 of this part, and all other applicable requirements, as defined in § 202.401 of this part, implemented for restricted transactions;

(2) Must be independent and external; 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 data transactions;

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

(3) Examine relevant records required under § 202.1101 of this part;

(4) Examine the U.S. person's security requirements, as defined by § 202.248 of this part; 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 prohibited transactions, restricted transactions, and exempt transactions engaged in by the U.S. person;

(ii) Describe the methodology undertaken, including the policies and other documents reviewed, personnel interviewed, and any 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 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 were otherwise not effective in mitigating 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 of this part 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. 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 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 by any U.S. person that 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.

§ 202.1104 Reports on rejected prohibited transactions.

(a) *Who must report.* A report must be filed by any U.S. person that 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 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

§ 202.1104, 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.

(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 of this part.

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

(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 of this part.

(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.

(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.

(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.

Area ID	Latitude/longitude coordinates of geofenced area			
1	38.935624, −77.207888	38.931674, −77.199387	38.929289, −77.203229	38.932939, −77.209328
2	38.950446, −77.125592	38.952077, −77.120947	38.947468, −77.120060	38.947135, −77.122809
3	38.953191, −77.372792	38.953174, −77.369764	38.951148, −77.369759	38.951152, −77.372781
4	39.113546, −76.777053	39.131086, −76.758527	39.100086, −76.749715	39.093304, −76.760882
5	33.416299, −82.172772	33.416666, −82.164366	33.406350, −82.163645	33.406261, −82.172947
6	21.525093, −158.019139	21.525362, −158.002575	21.518161, −158.002233	21.518010, −158.018364
7	21.475012, −158.061844	21.483357, −158.057568	21.479226, −158.049881	21.472695, −158.052371
8	29.449322, −98.646174	29.452872, −98.637623	29.448069, −98.637303	29.444547, −98.640607

Dated: October 18, 2024.

Matthew G. Olsen,

Assistant Attorney General for National Security, U.S. Department of Justice.

[FR Doc. 2024–24582 Filed 10–22–24; 4:15 pm]

BILLING CODE 4410–PF–P