DEPARTMENT OF JUSTICE

28 CFR Part 202

[Docket No. NSD 104]

RIN 1124–AA01

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: Final rule.

SUMMARY: The Department of Justice is issuing a final 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: This rule has been classified as meeting the criteria under 5 U.S.C. 804(2) and is effective April 8, 2025. However, at the conclusion of the Congressional review, if the effective date has been changed, the Department of Justice will publish a document in the **Federal Register** to establish the actual date of effectiveness or to terminate the rule. The incorporation by reference of certain material listed in this rule is approved by the Director of the Federal Register as of April 8, 2025.

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:

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.[1]

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

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.[2] On October 29, 2024, the Department issued a Notice of Proposed Rulemaking (''NPRM'') to address the public comments received on the ANPRM, set forth a proposed rule to implement the Order, and seek further public comment.[3] The Department is now issuing a final rule that addresses the public comments received on the NPRM and that implements the Order. The rule identifies classes of prohibited and restricted transactions; identifies countries of concern and classes of covered persons with whom the regulations 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.

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.[4] 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 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; and to take whatever additional actions, including promulgating additional regulations, as may be necessary to carry out the purposes of the Order.

The 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 to such data and present an unacceptable risk to U.S. national security. The rule (1) identifies certain classes of highly sensitive transactions with countries of concern or covered persons that the rule prohibits 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 or covered persons. As the Department discussed in the NPRM, the Attorney General has determined that the prohibited and restricted transactions set forth in the 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 rule identifies certain classes of transactions that are exempt from the rule. For example, the 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 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 rule also establishes a compliance and enforcement regime.

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

The Order and this 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.'' [5] As the NPRM 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

[2] 89 FR 15780 (Mar. 5, 2024).

[3] 89 FR 86116 (Oct. 29, 2024).

[4] 89 FR 15421.

[5] *Id.*

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.'' [6] 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.'' [7]

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.[8]

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 AI-driven analytics, will enable [the People's Republic of China (''China'' or ''PRC'')] to automate the identification of individuals and groups beyond China's borders to target with propaganda or censorship.'' [9]

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.'' [10] The study further explained that location datasets could reveal ''U.S. military bases and undisclosed intelligence sites'' or ''be used to estimate military population or troop buildup in specific areas around the world or even identify areas of off-base congregation to target.'' [11] 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.[12] 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.[13] The Order and this 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.

Additional open-source reporting released since issuance of the NPRM underscores the increasingly urgent risks posed by countries of concern obtaining access to government-related data or bulk U.S. sensitive personal data. For example, on November 22, 2024, cybersecurity researchers presented their findings after monitoring a collection of black-market services that recruit and pay insiders from a wide range of Chinese information technology (''IT''), technology, telecom, and other companies, to sell their access to individuals' data to online buyers. As a result, according to the researchers, these black-market services create an ecosystem for the public to pay to query individuals' data, including call records, bank accounts, hotel bookings, flight records, passport images, and location data.[14]

On November 19, 2024, WIRED released the results of an investigation in which they bought the digital advertising data and location information on phones in Germany from a U.S. data broker and used it to track the movements of United States Government contractors, intelligence personnel, and soldiers.[15] The investigation uncovered and tracked ''38,474 location signals from up to 189 devices *inside* Büchel Air Base, a high-security German installation where as many as 15 U.S. nuclear weapons are reportedly stored in underground bunkers''; 191,415 signals from up to 1,257 devices at Grafenwöhr Training Area, ''where thousands of U.S. troops are stationed and have trained Ukrainian soldiers on Abrams tanks''; and 164,223 signals from nearly 2,000 devices at Ramstein Air Base, ''which supports some U.S. drone operations.'' [16] The researchers observed patterns that went ''far beyond just understanding the working hours of people on base,'' including ''map[ping] key entry and exit points, pinpointing frequently visited areas, and even tracing personnel to their off-base routines.'' [17] As WIRED explained, ''foreign governments could use this data to identify individuals with access to sensitive areas; terrorists or criminals

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

[7] *Id.*

[8] 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*].

[9] 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*].

[10] 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*].

[11] *Id.*

[12] 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*).

[13] *Id.*

[14] Andy Greenberg, *China's Surveillance State Is Selling Citizen Data as a Side Hustle,* WIRED (Nov. 21, 2024), *https://www.wired.com/story/chinese-surveillance-state-is-selling-citizens-data-as-a-side-hustle/* [*https://perma.cc/9B9P-3ZR6*].

[15] Dhruv Mehrotra & Dell Cameron, *Anyone Can Buy Data Tracking US Soldiers and Spies to Nuclear Vaults and Brothels in Germany,* WIRED (Nov. 19, 2024), *https://www.wired.com/story/phone-data-us-soldiers-spies-nuclear-germany/* [*https://perma.cc/P5H6-3DFB*].

[16] *Id.*

[17] *Id.*

could decipher when U.S. nuclear weapons are least guarded; or spies and other nefarious actors could leverage embarrassing information for blackmail.'' [18]

Similarly, on October 28, 2024, journalists found that ''the highly confidential movements of U.S. President Joe Biden, presidential rivals Donald Trump and Kamala Harris, and other world leaders can be easily tracked online through a fitness app that their bodyguards use,'' which tracked their precise location data even when they used the app while off-duty.[19] This rule will prevent such foreign adversaries from legally obtaining such data through commercial transactions with U.S. persons, thereby stemming data flows and directly addressing the national security risks identified in the Order.

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 (''PADFAA'') do not create a comprehensive regulatory scheme that adequately and categorically addresses these national security risks,[20] as explained in part IV.L 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.'' [21] However, 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.[22]

Similarly, Executive Order 13873 prohibits any acquisition, importation, transfer, installation, dealing in, or use by U.S. persons of 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.'' [23] 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.'' [24] 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 rule complements 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 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 rule addresses 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. Rulemaking Process

The Department has issued this rule via notice-and-comment rulemaking consistent with the President's direction in the Order, and it has provided the public with multiple and meaningful opportunities to share feedback on the rule at various stages of the rulemaking process.[25] On March 5, 2024, the Department issued a fulsome ANPRM setting forth the contemplated contours of the rule, posed 114 specific questions for public input, and allotted 45 days for public comment.[26]

As described in the NPRM, the Department also solicited input on the ANPRM through dozens of large-group listening sessions, industry engagements, and one-on-one engagements with hundreds of participants.[27] 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

[18] *Id.*

[19] Sylvie Corbet, *Fitness App Strava Gives Away Location of Biden, Trump and Other Leaders, French Newspaper Says, Associated Press* (Oct. 28, 2024), *https://apnews.com/article/biden-trump-macron-bodyguards-security-strava-0a48afca09c7aa74d703e72833dcaf72* [*https://perma.cc/W59P-Y6TY*].

[20] *See* Public Law 118–50, div. I, 118th Cong. (2024).

[21] 50 U.S.C. 4565(a)(4)(B)(iii)(III).

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

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

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

[25] This 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. 553(a)(1). The 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 rule has 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 U.S. sensitive personal data). Although the rule is not subject to the APA's notice and comment requirements, the Department is engaging in notice-and-comment rulemaking for this rule, consistent with sections 2(a) and 2(c) of the Order.

[26] 89 FR 15780.

[27] 89 FR 86119–56.

Commerce, Tesla, Workday, Anthropic, and the Special Competitive Studies Project. It also 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 of Justice 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, as well as through other public engagements such as the Lawfare Podcast, ChinaTalk Podcast, CyberLaw Podcast, and the Center for Cybersecurity Policy & Law's Distilling Cyber Policy podcast.

During the ANPRM comment period, the Department received 64 timely comments, including 15 comments from trade associations; 13 from non-profits; three from advocacy associations; three from technology companies; two from think tanks; and one each from an automobile manufacturer, advertising company, biotechnology company, and academic medical center. The Department also received two comments after the close of the ANPRM comment period. In turn, the NPRM included a lengthy and substantive consideration of these timely and untimely public comments received on the ANPRM.[28]

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. These commenters included the Council on Government Relations Industry Association; the Association of American Medical Colleges; Airlines for America; the Bank Policy Institute; the Business Roundtable; the Information Technology Industry Council; the Centre for Information Policy Leadership; the Biotechnology Innovation Organization; the Software and Information Industry Association; the Cellular Telephone Industries Association; the internet and Television Association; USTelecom; Ford Motor Company; the Bioeconomy Information Sharing and Analysis Center; the Coalition of Services Industries; the Enterprise Cloud Coalition; the Electronic Privacy Information Center; the Center for Democracy and Technology; the Business Software Alliance; the Global Data Alliance; the Interactive Advertising Bureau; the U.S.-China Business Council; IBM, Workday; and individuals Justin Sherman, Mark Febrizio, and Charlie Lorthioir. The Department 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 published an NPRM on October 29, 2024, that addressed the public comments received on the ANPRM, set forth draft regulations and a lengthy explanatory discussion, and sought public comment.[29] During the NPRM comment period, the Department, 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 NPRM. Also during the NPRM comment period, the Department, in coordination with the Department of Commerce, conducted individual consultations with the Pharmaceutical Research and Manufacturers of America, the Centre for Information Policy Leadership, the Electronic Privacy Information Center, the Information Technology Industry Council, the World Privacy Forum, the U.S. Chamber of Commerce, the Council on Government Relations, BSA The Software Alliance, and the Telecommunications Industry Association to discuss their members' views. In accordance with 28 CFR 50.17, the Department has documented all ex parte engagements during the NPRM's comment period and publicly posted summaries of them on the docket for this rulemaking on *regulations.gov*. The Department encouraged those groups to submit detailed, timely comments to follow up on those discussions. The Department also discussed the NPRM with stakeholders at events open to the public, including ones hosted by the American Conference Institute, and through other public engagements such as the Lawfare Podcast, ChinaTalk Podcast, and the Center for Cybersecurity Policy & Law's Distilling Cyber Policy podcast. The Department also discussed the NPRM with foreign partners to ensure that they understood the contemplated program and how it fits into broader national security, economic, and trade policies.

Although the NPRM evolved from the ANPRM based on the Department's consideration of public comments, such as by adding new potential exemptions to the proposed rule's prohibitions and restrictions, the NPRM included most of the substantive provisions that the Department either previewed or described in detail in the ANPRM. For example, in many instances, the NPRM adopted without change definitions the Department also set forth in the ANPRM.[30]

The Department received and carefully reviewed 75 timely comments in response to the NPRM from trade associations, public interest advocacy groups, think tanks, private individuals, and companies, as well as comments from several foreign governments. The Department also reviewed three comments that were relevant to the NPRM and that were timely filed on the docket in response to the Cybersecurity and Infrastructure Security Agency (''CISA'') **Federal Register** notice requesting comment on proposed security requirements applicable to restricted transactions.[31] The Department considered each comment that was timely submitted.

During the 31-day comment period, the Department received a request to extend the time allotted for public comment.[32] As described in the NPRM, the Department solicited input on the ANPRM through engagements with dozens of stakeholders, including many of the commenters who sought the extension to the NPRM comment period.[33] As described in detail in part III of this preamble, during the NPRM comment period, the Department also conducted numerous engagements with the public to facilitate meaningful public participation during the comment period by providing stakeholders with an opportunity to ask questions about the proposed rule and to provide relevant feedback. These engagements included the organizations that requested that the Department extend the comment period.

The Department considered this request but declined to extend the comment period for several reasons.[34]

[28] *Id.*

[29] 89 FR 86116.

[30] *See, e.g.,* 89 FR 86123.

[31] 89 FR 85976 (Oct. 29, 2024).

[32] Consumer Tech. Ass'n, et al., Comment Letter on Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Gov't-Related Data by Countries of Concern or Covered Persons (Nov. 8, 2024), *https://www.regulations.gov/comment/DOJ-NSD-2024-0004-0008* [*https://perma.cc/3URP-9H7B*]. Although the official comment period was 30 days from the NPRM's publication in the **Federal Register** on October 29, 2024, the Department shared the NPRM on its website on October 21, 2024, providing the public with a total of 41 days to review and provide comment. *See* Press Release, U.S. Dep't of Just., *Justice Department Issues Comprehensive Proposed Rule Addressing National Security Risks Posed to U.S. Sensitive Data* (Oct. 21, 2024), *https://www.justice.gov/opa/pr/justice-department-issues-comprehensive-proposed-rule-addressing-national-security-risks* [*https://perma.cc/ZS7G-9QZH*].

[33] 89 FR 86119–56.

[34] U.S. Dep't of Just., Comment Letter on Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Gov't-Related Data by

As the Order, ANPRM, NPRM, and part IV of this preamble describe, the Department is issuing this rule to address the national emergency posed by an unusual and extraordinary threat from the continued effort of countries of concern to access government-related data and bulk U.S. sensitive personal data. This is an increasingly urgent threat, and the Department must move expeditiously to address it. Foreign adversaries are actively trying to exploit commercial access to Americans' sensitive personal data to threaten U.S. national security. This rule thus fills what Members of Congress and Administrations of both parties have consistently recognized is a significant gap in U.S. national security.

For example, the 2017 National Security Strategy noted that China and other adversaries ''weaponize information'' against the United States and predicted that ''[r]isks to U.S. national security will grow as competitors integrate information derived from personal and commercial sources with intelligence collection and data analytic capabilities based on Artificial Intelligence (AI) and machine learning.'' [35] That strategy criticized ''U.S. efforts to counter the exploitation of information'' by adversaries as ''tepid and fragmented,'' having ''lacked a sustained focus.'' [36] A partially declassified April 2020 assessment by the Office of the Director of National Intelligence (''ODNI'') explained that foreign adversaries are ''increasing their ability to analyze and manipulate large quantities of personal information in ways that will allow them to more effectively target and influence, or coerce, individuals and groups in the United States and allied countries.'' [37] The 2022 National Security Strategy underscored the need to develop a way to ''counter the exploitation of Americans' sensitive data.'' [38] A bipartisan 2023 report by the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party (''CCP'') explained that the ''CCP is committed to using the presence of technology products and services it controls to conduct cyberattacks on the United States,'' ''collect data on Americans to advance its AI goals,'' and ''surveil Americans as part of its campaign of transnational repression.'' [39] The Committee's bipartisan recommendations included taking ''steps to prevent foreign adversaries from collecting or acquiring U.S. genomic and other sensitive health data.'' [40] The 2024 National Counterintelligence Strategy made protecting Americans against foreign intelligence targeting and collection a key goal given foreign adversaries' ''broader focus on data as a strategic resource'' and the counterintelligence value it provides.[41] The November 2024 Report to Congress of the U.S.–China Economic & Security Review Commission explained that ''China understands the value of data to AI and has taken active measures to increase the availability of quality data within its AI ecosystem.'' [42] The report also explains that the ''major research and market presence of Chinese genomic and biotech services companies in the United States gives these companies access to key technologies and data,'' leading to a ''heightened risk of the transfer of sensitive health data of U.S. citizens'' to China.[43] And so on.

Extending the comment period would allow this increasingly urgent, unaddressed threat to continue unabated, giving countries of concern more time and opportunities to collect and exploit government-related data and bulk U.S. sensitive personal data.[44] Delay only increases this unusual and extraordinary threat which gives countries of concern ''a cheap and reliable way to [among other threatening activities] track the movements of American military and intelligence personnel overseas, from their homes and their children's schools to hardened aircraft shelters within an airbase where . . . nuclear weapons are believed to be stored.'' [45] Not only do countries of concern like China ''draw on . . . commercially collected data sources . . . [and] insiders from the country's tech and telecom firms [and] banks'' to perpetuate its surveillance apparatus, they also sell their access to such data for other nefarious purposes that can put Americans at risk.[46]

The Department also believes that extending the comment period would not provide meaningful additional input that would improve the rule. The Department has gone to great lengths to provide the public with meaningful opportunities to provide input at every stage of development of this rule. The Department took the optional step of releasing an ANPRM to provide the public with an additional formal opportunity to comment, in addition to the public's formal opportunity to comment on the NPRM. The rule closely tracks the NPRM, which had all its core components extensively previewed in the ANPRM. The public has had at least 87 days to formally provide comments throughout this rulemaking: The comment period on the NPRM was 31 days, the public had an additional 11 days to review the NPRM while it was on public inspection in the **Federal Register** before it was formally published, and the public had 45 days to comment on the ANPRM.

In addition to these formal opportunities to comment, and as documented in the ANPRM, NPRM, part III of this preamble, and the docket on *regulations.gov,* the Department also provided extensive informal opportunities for feedback. Those opportunities began with multiple informal engagements with hundreds of stakeholders before the release of the Order and ANPRM. After the release of the ANPRM and NPRM, the Department undertook extensive large-group, small-group, and one-on-one engagements with over 800 stakeholder invitees or participants across over 50 informal engagements to explain the rule and provide feedback.

Countries of Concern or Covered Persons (Nov. 18, 2024), *https://www.regulations.gov/document/DOJ-NSD-2024-0004-0028* [*https://perma.cc/M86F-5NUG*].

[35] Exec. Off. Of the President, *National Security. Strategy of the United States of America* 34 (Dec. 2017), *https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf* [*https://perma.cc/R4F5-QXJH*].

[36] *Id.* at 35.

[37] Nat'l Intel. Council, *supra* note 9, at 3.

[38] Exec. Off. of the President, *National Security Strategy* 33 (Oct. 12, 2022), *https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf* [*https://perma.cc/G54X-L7ER*].

[39] H. Select Comm. on the Strategic Competition Between the U.S. and the Chinese Communist Party, *Reset, Prevent, Build: A Strategy to Win America's Economic Competition with the Chinese Communist Party* 22 (2023), *https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/reset-prevent-build-scc-report.pdf* [*https://perma.cc/5A7Q-YL9U*].

[40] *Id.* at 23.

[41] Nat'l Counterintel. & Sec. Ctr., *supra* note 6, at 13.

[42] U.S.-China Econ. & Sec. Review Comm'n, 118th Cong., 2024 Rep. to Cong. 11 (Comm. Print 2024), *https://www.uscc.gov/sites/default/files/2024-11/2024_Annual_Report_to_Congress.pdf* [*https://perma.cc/ZWC5-G5SV*].

[43] *Id.* at 12, 220.

[44] *See, e.g.,* Mehrotra & Cameron, *supra* note 15 (describing an ''analysis of billions of location coordinates obtained from a US-based data broker [that] provides extraordinary insight into the daily routines of US service members'' and ''[provides]'' ''a vivid example of the significant risks the unregulated sale of mobile location data poses to the integrity of the US military and the safety of its service members and their families overseas'').

[45] *Id.*

[46] *See* Greenberg, *supra* note 14 (describing how a surveillance data black market has developed in China due in part to there being ''virtually no legal checks on the government's ability to physically and digitally monitor its citizens'' and in which ''phone numbers, hotel and flights records, and . . . location data [are sold]'' in criminal markets).

As described in part IV of this preamble, many of the comments received on the NPRM merely state preferences or renew comments made on the ANPRM without providing specific information or new analysis, or do not engage with the analysis in the NPRM. The constructive refinements suggested by commenters have become increasingly discrete. In addition, many commenters have not specifically identified what additional changes, analysis, or data they would provide if given additional time to comment. The Department thus believes that the opportunities for public comment and input during this rulemaking process have appropriately balanced the need for feedback to ensure that the rule effectively addresses the national security risks and the need to move expeditiously given the increasingly urgent national security risks.

IV. Discussion of Comments on the Notice of Proposed Rulemaking and Changes From the Proposed Rule

The discussion in part IV of this preamble summarizes comments submitted in response to the NPRM and responds to those comments. The Department does not discuss provisions of the rule that commenters did not address substantively and has implemented those provisions in the final rule without change from the NPRM. Unless the Department otherwise addresses parts of the rule in this preamble, the Department incorporates the NPRM's discussion of the rule into the preamble,[47] including, for example, the Department's determination that the categories of covered data transactions pose an unacceptable risk to national security,[48] the Department's interpretation of ''information or informational materials'' under IEEPA,[49] and the Department's analysis for proposed bulk thresholds.[50]

Many comments were constructive. They expressed strong support for the goals of the Order and the rule, the use of exemptions as a careful and targeted approach to addressing the national security and foreign policy risks, and the Department's changes in the NPRM in response to comments on the ANPRM. These comments suggested and justified additional specific refinements that help clarify and reinforce the targeted nature of the Order and the rule, which are addressed with respect to the relevant subparts of the rule.

Some commenters suggested clarifications or changes that were premised on a misunderstanding or narrow view of the Order and this rule. For example, some comments were premised on the view that the national security and foreign policy risks addressed by the Order and this rule are solely or primarily about the identifiability of a set of sensitive personal data. As the NPRM explained, anonymized data is rarely, if ever, truly anonymous, especially when anonymized data in one dataset can become identifiable when cross-referenced and layered on top of another anonymized dataset.[51] In addition, as the Department discussed in detail in the NPRM, identifiability is only one in a range of concerns. Anonymized data itself can present a national security risk, as can pattern-of-life data and other insights that harm national security from anonymized data itself (such as in the case of precise geolocation data).[52] Sets of bulk U.S. sensitive personal data may also be used to identify vulnerabilities within a population or, in the case of bulk human genomic data, to enhance military capabilities that include facilitating the development of bioweapons. Additionally, even smaller sets of bulk U.S. sensitive personal data can be used to make statistical inferences or conclusions about much larger population sets. Usually, a sample size should not and need not exceed 10 percent of a population to make inferences about the entire population. However, even extremely small sample sizes may allow the extrapolation of inferences about much larger populations. For example, Meta requires only a source audience of 1,000 customers, which need only include 100 people from a single country, in order to extrapolate a ''lookalike'' audience of million individuals for targeted advertising. In other words, countries of concern may be able to glean valuable information about the health and financial well-being of a large number of Americans through smaller datasets of bulk U.S. sensitive personal data. As a result, the Department has not adopted these suggestions, as they do not account for the broader range of national security risks that the Order and this rule address.

Similarly, some comments were premised on a narrow view that the sole or primary focus of the rule is the sale of data. As discussed at length in the Order, ANPRM, and NPRM and as further described in part IV.C of this preamble, the sale of data is only one means by which countries of concerns are seeking access to government-related data and bulk U.S. sensitive personal data. Countries of concern also leverage vendor, employment, and investment agreements as additional vectors to try to obtain that access. As a result, the Department has not adopted suggestions to the extent that they do not account for the full range of risk vectors that the Order and this rule addresses.

Many comments failed to provide specifics the Department would need to justify changes to the rule. These comments merely stated policy preferences or made conclusory assertions without providing meaningful support or analysis, or without addressing the analysis in the ANPRM and NPRM. For example, some comments claimed that the rule would have particular impacts on certain sectors or activities, but they did not identify specific non-exempt covered data transactions with countries of concern or covered persons that currently occur that the rule would prohibit or restrict, explain the significance of these transactions to the sector or industry, show why the sensitive personal data in those transactions was integral to share with a country of concern or covered person, or explain why it would not be feasible to shift those transactions to other countries or persons over time.

Other comments reflected misunderstandings about the Order and the proposed rule. For example, several comments stated that, with respect to different provisions of the proposed rule that apply to a category of activity ''including'' a list of specifics, it is unclear whether those lists are exhaustive or exemplary. There is no ambiguity, however, because § 202.102(b) already defines ''including'' to mean ''including but not limited to.'' The final rule addresses other mistaken assertions and misunderstandings with respect to each subpart in part IV of this preamble and clarifies what the rule does or does not do.

One commenter reiterated comments originally provided on the ANPRM to suggest that the Order's and the proposed rule's restrictions on access to sensitive personal data are inconsistent with international commitments by the United States. Specifically, the commenter calls on the Department to make a greater effort to explain how the rule is consistent with the U.S. commitment towards the promotion of trusted cross-border data flows. As the NPRM explained, the rule permits cross-border data flows except with respect to

[47] 89 FR 86117–70.

[48] 89 FR 86121.

[49] 89 FR 86165–70.

[50] 89 FR 86156–65.

[51] 89 FR 86126–27.

[52] *Id.*

commercial transactions that pose unacceptable national security risks (and thus lack the trust required for the free flow of data), which the rule prohibits or restricts.[53] Because the commenter merely renews its prior comment on the ANPRM without any attempt to address the explanation in the NPRM, no further explanation appears necessary.

The Department will continue to assess the risk posed by countries of concern and covered persons accessing government-related data or bulk U.S. sensitive personal data, including examining whether the Department needs to expand the final rule to tackle connected data security concerns, such as data scraping or illegitimate data access via the provision of services from entities linked to state threat actors. The Department retains the right to promulgate additional rules within the scope of the Order to address that risk.

Two commenters reiterated suggestions that the Department make various revisions to borrow or incorporate aspects of international or State privacy laws into this rule. As previously stated in the NPRM, the Department supports privacy measures and national security measures as complementary protections for Americans' sensitive personal data.[54] 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. Commenters' suggestions raise no new justifications that the Department did not already consider at the NPRM stage, nor do these suggestions address how or why privacy protections would adequately address national security concerns such that the Department should align definition with existing privacy laws.

In response to the NPRM, 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. One commenter requested that the Department exempt disclosures of nonclinical research data where research subjects consented to the disclosure of their data. Another commenter expressed concern about their data being sold within the United States for commercial purposes without consent or equitable benefit.

The rule declines to adopt a consent exemption for the same reasons provided in the NPRM. As explained in the NPRM, 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 bulk U.S. sensitive personal data with countries of concern or covered persons.[55] It is precisely those choices that, in aggregate, have helped create the national security risk of access by countries of concern or covered persons, and the purpose of the Order and the rule is to address the negative externality that has been 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 rule does 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.

The Department also declines to adopt a residual compensation requirement for domestic sales of data. The Order and this rule do not address purely domestic transactions between U.S. persons—such as the collection, maintenance, processing, or use of data by U.S. persons within the United States—except to the extent that such U.S. persons are affirmatively and publicly designated as covered persons.

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

A. General Comments

1. Section 202.216—Effective Date

The NPRM did not propose a specific effective date of the applicable prohibitions and directives contained in the proposed rule. One commenter requested consultation with the Department on a timeframe for the implementation of the final rule. Some commenters requested that the Department delay the effective date of the rule—with requests ranging from 12 months to 18 months, or an indefinite deadline—to allow companies, individuals, and universities time to assess their data transactions, update internal polices, make necessary data security changes, and come into compliance without disrupting commercial activity. Two commenters suggested that the Department ''pause'' rulemaking, postpone publication of the final rule, or, alternatively, publish the regulations for prohibited transactions first and postpone the publication of restricted transactions to a later, indeterminate date to provide more time for consultation and revisions to those provisions.

The Department carefully considered these requests and declines, at least at this time, to categorically extend the effective date beyond April 8, 2025. The Department will, however, delay the date for when U.S. persons must comply with subpart J, related to due diligence and audit requirements for restricted transactions, and for §§ 202.1103 and 202.1104, related to certain reporting requirements for restricted transactions, until October 6, 2025.

For reasons similar to the reasons why the Department declined to extend the comment period, the Department declines these commenters' request to significantly delay the effective date across the board. As the Order, ANPRM, NPRM, and parts III and IV of this preamble explain, this rule addresses a national emergency and an unusual and extraordinary threat to national security and foreign policy. Foreign adversaries are actively trying to exploit commercial access to Americans' sensitive personal data to threaten U.S. national security. This threat is increasingly urgent, justifying the expedited process for this rulemaking to address that threat. Significantly delaying the effective date of the final rule across the board would

[53] 89 FR 86121.

[54] *Id.*

[55] *Id.*

give countries of concern additional time to collect government-related data and bulk U.S. sensitive personal data.[56] The pressing risks posed by these countries' ongoing attempts to collect and exploit government-related data and bulk U.S. sensitive personal data to the detriment of U.S. national security weigh against extending the effective date of the rule, notwithstanding the compliance burdens some commenters raised. Commenters' request for a significantly delayed effective date cannot be reconciled with the need to expeditiously address these increasingly urgent and serious risks. United States persons have been on notice regarding the risks of sharing sensitive personal data with countries of concern for years and the United States Government's recommended steps to address those risks. For example, since at least 2020, the Department of Homeland Security (''DHS'') has publicly warned U.S. businesses using data services from the PRC or sharing data with the PRC about the same risk vectors addressed by this rule.[57] DHS Security has urged U.S. entities to ''scrutinize any business relationship that provides access to data'' by ''identifying the sensitive personal and proprietary information in their possession,'' ''minimiz[ing] the amount of at-risk data being stored and used in the PRC or in places accessible by PRC authorities,'' and conducting ''[r]obust due diligence and transaction monitoring'' that includes ''acquir[ing] a thorough understanding of the ownership of data service providers, location of data infrastructure, and any tangential foreign business relationships and significant foreign investors.'' [58]

United States persons have been aware of this contemplated rulemaking since the issuance of the Order and ANRPM in February 2024. During engagements with companies and industry, some participants suggested that their efforts to understand and map their covered data transactions are already underway, and some other multinational companies explained that they already operate separate systems that ''firewall'' U.S.-person data from access in China and other countries of concern and impose access controls to prevent unauthorized foreign access. Similarly, in the comments on the NPRM, a different large global technology business stated that multinational companies already have robust data privacy and export control programs that may be leveraged to comply with the rule, and that companies should not be required to set up entirely new compliance programs; another commenter echoed the view that companies should be able to leverage existing privacy and data security programs. But given the serious national security concerns, if the rule becomes effective, for example, before a U.S. person engaging in restricted transactions is able to comply with the security and other requirements the U.S. person should not engage in those transactions.

The comments seeking to significantly delay or pause the effective date did not offer adequate substantive analysis or support necessary to justify the change. These comments expressed a general preference for delay, but they did not attempt to, for example, identify what and how many specific non-exempt transactions they engage in that would be prohibited or restricted; identify what specific controls, recordkeeping, or systems they currently have in place and why those are not sufficient to comply; identify what controls, recordkeeping, or systems they do not have in place now that they would be required to adopt to comply with the rule; or explain why those transactions could not be paused, terminated, or shifted to non-countries of concern or non-covered persons before the effective date or the specific impact of doing so. The Department thus does not believe that these comments provide an adequate basis on which to justify a significantly delayed effective for the sectors and industries represented by the commenters, in light of the pressing national security risks described in the Order, ANPRM, NPRM, and this preamble.

In addition, the commenters requesting a significantly delayed effective date represent specific sectors and industries. The specific industries represented by these commenters appear to have different views about the time and resources needed for implementation and do not appear to be sufficiently representative of the entire category of U.S. persons engaging in data transactions that may be prohibited or restricted under the rule. The Department thus does not believe that these comments justify an across-the-board delay of the effective date.

As a result, in light of the need to expeditiously address the increasingly urgent national security threat and the lack of significant and specific countervailing evidence, the Department believes that it is appropriate for the final rule to establish an effective date of 90 days as a starting point, consistent with 5 U.S.C. 801(a)(3) and 5 U.S.C. 553(d).[59] At one end of the spectrum, an earlier effective date may mean more U.S. persons are not prepared to comply with the rule and who must delay (or forgo, in some cases) transactions that may implicate the rule or forgo a broader suite of business opportunities that would not be prohibited or restricted under the rule, resulting in temporary but additional costs while they prepare to comply. At the other end of the spectrum, a later effective date would mean a greater risk to national security and foreign policy while countries of concern and covered person have additional time to access, obtain, and exploit government-related data or bulk U.S. sensitive personal data. The Department believes it is appropriate to err on the side of the former given the serious and pressing risks.

The Department recognizes that U.S. persons may need time to amend internal policies and procedures to ensure compliance with the final rule's due diligence provisions and to comply with reporting requirements by, for example, evaluating and assessing ongoing transactions or transaction types. Some aspects of the rule can be delayed without unduly compromising the national security interests advanced by the principal prohibitions and restrictions in subparts C and D. The rule's due-diligence requirements for engaging in restricted transactions and the recordkeeping requirements that apply to both prohibited and restricted transactions are based on existing compliance expectations set by other

[56] *See, e.g.,* Mehrotra & Cameron, *supra* note 15 (describing an ''analysis of billions of location coordinates obtained from a US-based data broker [that] provides extraordinary insight into the daily routines of US service members'' and provides ''a vivid example of the significant risks the unregulated sale of mobile location data poses to the integrity of the US military and the safety of its service members and their families overseas'').

[57] U.S. Dep't of Homeland Sec., *Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to China, https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf* [*https://perma.cc/2C5B-CEWC*].

[58] *Id.* at 13.

[59] These provisions—in particular 5 U.S.C. 801(a)(3)—generally require the effective date be at least 60 days after publication of the rule in the **Federal Register**. The Department has not invoked any exception to these statutory requirements, notwithstanding the national emergency and threat to national security and foreign policy addressed by this rule. Although the risks addressed by this rule are urgent and ongoing, the Department recognizes the breadth of potential disruption to current business activities and the associated economic interest in a more orderly process for coming into compliance with this rule. The Department is exercising its discretion in balancing the ongoing threats to national security with the potential disruption to current business activities and has therefore determined that while a blanket extension beyond 90 days is unwarranted, it also would not be appropriate to establish an effective date earlier than that.

regulators, such as the Department of Treasury's Office of Foreign Asset Control (''OFAC'') and the Department of Commerce's Bureau of Industry and Security (''BIS''), for screening vendors and transaction counterparties. The Department recognizes, however, the specific burden in applying these provisions to this new context, and has determined it is appropriate to allow additional time—an additional six months—before those provisions become operative. Thus, the provisions in §§ 202.1001, 202.1002, 202.1103, and 202.1104 will only apply to those who engage in the relevant transactions (or, for § 202.1104, reject a proposed transaction) on or after October 6, 2025. The Department believes that this will allow sufficient time for the vast majority of entities to come into compliance with these provisions and appropriately balances the value of these provisions to combatting the national security threat they are intended to address. This delay will have the effect of phasing in these additional compliance requirements, allowing U.S. persons to focus their efforts at the start on identifying and understanding the data transactions they engage in and complying with the prohibitions and restrictions.

During the 90-day period before the rule's effective date and the additional period before the remaining provisions become operative, the Department will continue to robustly engage with stakeholders to determine whether additional time for implementation is necessary and appropriate. Through those engagements and with more specific information, the Department may determine, for example, that it is appropriate (1) for the 90-day effective date to remain in effect, but to issue a general license authorizing companies to take additional time to wind-down activities regulated by the rule if they cannot come into compliance before that date; (2) for the 90-day effective date to remain in effect, but to issue a general license establishing delayed effective dates for specific sectors or activities; (3) for the 90-day effective date to remain in effect, but to issue a general license further delaying the effective date as to certain compliance requirements or adjusting those requirements; (4) for the 90-day effective date to remain in effect, but to issue a non-enforcement policy for a certain period; (5) to delay the effective date, either through regulatory modification or a general license; or (6) to make no changes. The Department will also consider other courses of action as circumstances warrant.

Several commenters requested that the Department incorporate a mechanism for continued engagement with the public to discuss and assess the rule's effectiveness in light of, and its application to, evolving technologies and threats and to provide compliance guidance. After the Department issues the final rule, the Department plans to continue its robust stakeholder engagement, as it has done throughout the rulemaking process, and issue guidance on compliance and other topics. In addition, through the advisory opinion process, the rule provides a formal avenue for the public to request and receive clarifications about the rule's applicability to particular transactions. Finally, section 5 of the Order already establishes a formal mechanism for the Department to assess the effectiveness and economic impact of the rule by requiring a report within one year after the rule goes into effect, which will include the solicitation and consideration of public comments.[60]

A few commenters requested clarification from the Department on whether the provisions of the rule will apply retroactively and to existing contracts, or if the provisions will only apply prospectively on new contracts or contracts up for renewal. One commenter requested that if the Department determines that retroactive application is required for the provision in § 202.302 requiring certain contractual provisions for data brokerage transactions with foreign persons, then the Department allow sufficient time to amend existing agreements to ensure compliance.

The rule applies to covered data transactions engaged on or after the effective date. Covered data transactions completed prior to the effective date are not regulated by the rule. However, unless exempt or otherwise authorized, U.S. persons knowingly engaging in a prohibited or restricted covered data transaction on or after the effective date are expected to comply with the rule, notwithstanding any contract entered into or any license or permit granted before the effective date. In the case of § 202.302, for instance, this means that any relevant covered data transactions engaged in on or after the effective date must comply with the contractual requirements in § 202.302(a)(1), even where the U.S. persons had an existing agreement with the foreign person prior to the effective date. Restricted and prohibited transactions will not be grandfathered in as compliant simply because any resulting covered data transactions are subject to a preexisting contract or agreement. The significant national security concerns outlined in the Order, NPRM, and parts II–IV of this preamble require these regulations to be implemented as quickly as possible. Entities that believe they need more time to come into compliance with these regulations may request a specific license.

B. Subpart C—Prohibited Transactions and Related Activities

The proposed rule identified 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.'' [61] Pursuant to the Order, the proposed rule categorically prohibited or, for the categories of restricted transactions, imposed 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 defined 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. As stated in the NPRM, 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

[60] 89 FR 15427.

[61] 89 FR 15423.

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.'' [62]

Some commenters suggested that the final rule be limited to situations where government-related data or bulk U.S. sensitive personal data is made accessible by the U.S. person to the covered person or country of concern, and that it not apply in instances where (for example) a covered person sends bulk U.S. sensitive personal data to a U.S. person. The Department agrees that a U.S. person accessing data from a covered person ordinarily does not present the national security concerns that the rule seeks to address, and the Department does not intend the rule to cover that generic circumstance. Although commenters identified multiple ways to clarify this in the regulatory text, the Department clarifies this limitation by changing the definition of ''covered data transaction'' to cover only transactions that involve ''access by a country of concern or covered person.'' The rule includes a new example clarifying this limitation in § 202.210. This change also necessitates conforming changes to § 202.302 related to onward transfer provisions as explained in part IV.B.15 of this preamble.

Other commenters requested clarity about whether the rule would apply to other transactions that are related to a covered data transaction but that do not themselves provide a country of concern or a covered person access to bulk U.S. sensitive personal data or government-related data. The revised definition of ''covered data transaction'' captures only those transactions that involve access by a country of concern or covered person to bulk U.S. sensitive personal data or government-related data, as the term ''access'' is defined in the rule. The rule does not impose any restrictions or prohibitions on transactions that do not involve access by a country of concern or covered person to government-related data or bulk U.S. sensitive personal data. For instance, a U.S. research institution that entered into a vendor agreement with a covered person cloud-services provider in a country of concern to store bulk U.S. personal health data or bulk human genomic data in a country of concern would have to comply with the security requirements mandated by subpart D. But the rule would not impose any restrictions or prohibitions on the ability of U.S. or foreign persons who are not covered persons to access or analyze the bulk U.S. sensitive personal data stored by a country of concern cloud-services provider.

2. Section 202.301—Prohibited Data-Brokerage Transactions; Section 202.214—Data Brokerage

The NPRM proposed prohibiting 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 defined ''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.

Some comments expressed concern with the perceived breadth of the term ''data brokerage.'' These comments did not appropriately consider data brokerage in the context of the rest of the regulations (such as their exemptions, the other elements of the prohibitions and restrictions, and other related definitions that limit the scope and impact of data brokerage) and, as such, made exaggerated claims about its impacts without support or analysis. These comments were premised largely on imprecise hypotheticals or generalizations, or they misstated the regulations. In addition, none of these comments discussing data brokerage addressed the national security risk posed by countries of concern or covered persons accessing the digital footprint of sensitive personal data Americans leave behind when interacting with the modern world.

Nevertheless, the Department considered each such comment and responds to the themes presented in them in the continuing discussion. To the extent that such commenters reiterated points or suggestions that were already addressed in the NPRM, the Department directs those commenters to the relevant discussions in the NPRM.[63] Ultimately, the Department declines to make any changes to the prohibition in § 202.301, makes a limited change to the definition of ''data brokerage'' in § 202.214, adds three new examples to the definition, and amends one existing example.

Some commenters recommended that the Department adjust the definition of data brokerage to expressly exclude activities that are already subject to one of the proposed rule's exemptions to ensure the proposed regulations do not inadvertently capture transactions that are well-regulated by financial services regulators. No change was made in response to this comment. The exemptions in subpart E already explicitly make clear that the prohibitions and restrictions in ''subparts C and D do not apply to'' the categories of exempt transactions. And § 202.301 (the provision prohibiting certain data-brokerage transactions) already explicitly applies ''[e]xcept as otherwise authorized pursuant to subparts E or H of this part or any other provision of this part,'' which includes the exemptions in subpart E. Adding another reference to this issue would be redundant and unnecessary.

Some commenters expressed confusion about the supposed relationship or tension between data brokerage and vendor agreements, and suggested changes that would undermine the prohibitions and restrictions associated with those defined terms. For example, these commenters believed intra-company data transactions could be considered prohibited data brokerage but claimed that same transaction would only be restricted if engaged in pursuant to a vendor agreement. Some of these commenters and others also requested changes to the exemption for corporate group transactions in § 202.506 to address their confusion.

Data brokerage and vendor agreements are specifically tailored to address the risk to national security posed by a country of concern or covered person's access to government-related data or bulk U.S. sensitive personal data. While the commenters' hypothetical questions or concerns lack factual specificity, for additional clarity, the Department has amended the definition of ''data brokerage'' to explicitly exclude an employment, investment, or vendor agreement. This change helps ensure that the categories of prohibited transactions and restricted transactions remain mutually exclusive. Applying these definitions still involves a fact-specific analysis, as illustrated by

[62] Sherman et al., *supra* note 10, at 14.

[63] *See, e.g.,* 89 FR 86130–31.

the accompanying examples. The Department also added two new examples at §§ 202.214(b)(7) and (8) to further illustrate how companies primarily engaged in non-data brokerage activities might otherwise trigger the prohibition.

In addition, to the extent that intra-company or internal data transactions satisfy the exemption under § 202.506 because they are ordinarily incident to and part of administrative or ancillary business operations, those transactions would be exempt regardless of whether they are characterized as prohibited data brokerage or a restricted vendor agreement. Furthermore, after the effective date of the rule, the commenters and the broader public will have the opportunity to submit detailed requests for formal advisory opinions from the Department regarding any questions they have as to how these terms affect specific factual situations as opposed to hypothetical ones.

At least one commenter suggested that the Department amend the definition of ''data brokerage'' by omitting the ''licensing of access to data'' and ''similar commercial transactions'' prongs, and by limiting the scope to those transactions where sensitive data is exchanged for consideration. In the alternative, the commenter suggested that the Department narrow the scope to apply to the specific types of transactions the Department intends to cover. The commenter argued that the current definition of ''data brokerage'' is overbroad and extends beyond ''bulk sensitive personal data'' to all data, and that a broad interpretation of ''similar commercial transactions'' could expand the scope of compliance and impact actors in several sectors such as e-commerce and analytics firms. Other commenters suggested striking ''similar commercial transactions'' from the definition or amending it, including by adopting standards found in certain State privacy laws. And others asked the Department to reiterate concepts like ''sensitive personal data'' in the definition of data brokerage.

The Department declines to adopt these suggested approaches, parts of which were already discussed in the NPRM. The Department intends for the rule to cover a broad range of data brokerage transactions involving government-related data or bulk U.S. sensitive personal data. Persons selling or reselling data to others are engaging in data brokerage, even if such activity is not that person's primary business activity. As noted in the NPRM, the proposed rule intentionally covered both first- and third-party data brokerage because countries of concern do not discriminate in how they seek to access government-related data or bulk U.S. sensitive personal data. As such, the rule's broad definition is critical to ensuring there are no significant loopholes for countries of concern to continue to leverage the data brokerage market as a means of acquiring and exploiting government-related data or bulk U.S. sensitive personal data.

The Department also notes these comments appear to misapply data brokerage and its relationship to other provisions of the regulations. For example, the prohibition on data brokerage does not apply to all data. It only applies to covered data transactions, which, is limited to government-related data or bulk U.S. sensitive personal data. Adding sensitive personal data to the definition of the term would therefore be redundant. The phrase ''similar commercial transactions'' is intended to cover other commercial arrangements (beyond just sales and licensing) involving the transfer of government-related data or bulk U.S. sensitive personal data to countries of concern or covered persons. Commercial arrangements, by their nature, are engaged in for consideration. No further clarification of the phrase is warranted or necessary. Additionally, the exemption in § 202.505 regarding financial services already ensures that the term ''similar commercial transactions'' would not inadvertently capture e-commerce activities. Moreover, these comments' suggestions do not realistically describe how or whether their recommended approaches would mitigate the national security risk associated with the rule's examples of data-brokerage activities other than sale or licensing.

Another commenter suggested that to comply with the regulations, companies must first identify any data-brokerage activities they undertake, which the commenter claims is a daunting task. The commenter also warned that the definition would include activities beyond those engaged in by data brokerage firms. Many of the commenter's concerns were addressed in the preamble of the NPRM. The Department intends for data brokerage to encompass both first- and third-party data brokerage to address the national security risk the Order was intended to mitigate. That is a key national security feature of the program and is addressed earlier in part IV.B.2 of this preamble.

With respect to how to comply with the regulations, the Department does not endorse any specific practice. The Department believes it is more effective to have U.S. persons develop compliance programs suitable to their own individualized risk profile, as explained in the NPRM.[64] Such programs can vary based on a range 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. Without fully knowing the commenter's situation, alternative approaches to compliance may be appropriate, such as first evaluating the company's exposure to countries of concern or covered persons, or their possession of or access to government-related data or bulk U.S. sensitive personal data, to direct their compliance efforts.

At least two commenters proposed exempting data-sharing platforms from the definition of ''data brokerage'' because such platforms do not determine what data is shared or reviewed before data is shared. These commenters generally claimed that without the requested exemption, such platforms would be required to review all data exchanges and underlying datasets, potentially creating new privacy and data security risks as well as possible contractual violations. The Department declines to adopt this proposal because it is unnecessary, redundant, and risks creating an exemption that could inadvertently undermine the purpose of the rule, thereby exacerbating the national security risk the Order is intended to mitigate. The prohibition in § 202.301 requires ''knowingly'' engaging in a covered data transaction involving data brokerage with a country of concern or covered person. As the examples in §§ 202.230(b) and 202.305(b) illustrate, if a U.S. person merely provides infrastructure or a platform to a U.S. customer that uses the infrastructure or platform to engage in a prohibited or restricted transaction, the third-party infrastructure or platform provider would not generally have knowingly engaged in a prohibited or restricted transaction. However, it would be inappropriate for the rule to exempt third-party infrastructure or platform providers, as they could engage in their own transactions that would be prohibited or restricted, as also illustrated by the examples in § 202.230(b) and § 202.305(b).

At least two commenters were concerned that without changes to the definition of ''data brokerage'' or the prohibition in § 202.301, the regulations would adversely affect e-commerce or

[64] 89 FR 86128.

the ability of U.S. persons to purchase goods and services. These concerns are unfounded because the prohibition does not reach exempted activities, including data transactions that are ordinarily incident to and part of the provision of financial services. Financial services include ''the transfer of personal financial data or covered personal identifiers incidental to the purchase and sale of goods and services'' and ''the provision or processing of payments or funds transfers.'' *See* § 202.505(a)(4) and (5). Example 1 in § 202.505(b)(1) also specifically addresses the issue of e-commerce.

One comment expressed concern that U.S. persons engaged in data brokerage are unfairly targeted and encouraged the creation of a safe harbor for U.S. persons that conduct due diligence on data-brokerage transactions but are later deceived about a foreign adversary's ownership or control of a customer company. The Department declines to adopt the described safe harbor because it is unnecessary and redundant. The prohibition on data brokerage in § 202.301 requires a U.S. person to act ''knowingly,'' which ''means that a person has actual knowledge, or reasonably should have known, of the conduct, the circumstance, or the result.'' *See* § 202.230. Generally, U.S. persons engaged in data brokerage who are in fact deceived by countries of concern or covered persons, despite taking reasonable measures to comply with § 202.301, would not be liable because they would not have had actual knowledge of, nor would they have reasonably known of, the circumstances. In addition, the Department intends to issue compliance and enforcement guidance following the publication of the final rule.

Another commenter provided several open-ended hypotheticals about the applicability of the definition of ''data brokerage'' in § 202.214 to unfunded or nonprofit research. They asked whether a U.S. person's transfer of bulk sensitive personal data to a researcher in a country of concern could be considered data brokerage; whether such data transfers would be prohibited if they occurred because of mutual interest in the research; and whether the possibility of collaboration or co-authoring on a paper constitutes sufficient consideration to trigger the definition.

The public will have the opportunity to submit detailed requests for formal advisory opinions after the effective date of the regulations. In that process, filers would provide non-hypothetical and specific facts on which the Department will render an opinion on the applicability of the regulations. Without more specific information or details, the Department can only provide general answers to these hypotheticals.

As explained with respect to the comments on § 202.511, while the rule is not limited to covered data transactions that occur for solely commercial purposes, the rule does limit data brokerage and the other categories of covered data transactions (and thus the prohibitions and restrictions) to transactions that are commercial *in nature,* meaning that they involve some payment or other valuable consideration. Generally, without more, a mutual interest in conducting research together, or the possibility of research collaboration or co-authoring a paper, would not constitute the kind of valuable consideration needed to qualify as a covered data transaction. The Department added Examples 9 and 10 to § 202.214 to clarify the circumstances to which the Department intends the rule to apply in the context of such research activities.

Other commenters similarly sought clarification on whether and how the rule applies to nonprofit or non-commercial entities. The rule applies to data brokerage and investment, vendor, or employment transactions, as defined in the rule, without regard to the for-profit or not-for-profit nature of the U.S. person engaged in the transaction. Where a nonprofit engages in a covered data transaction—by, for example, entering a vendor agreement with a covered person to host bulk U.S. sensitive personal data—the rule applies. As the NPRM explained, the rule takes an activity-based approach because it is certain activities (transactions) that pose the unacceptable risks to national security and foreign policy, regardless of the kind of entity that engages in them.

However, other provisions of the regulations might exempt otherwise prohibited or restricted data transactions engaged in by researchers. The Department has exempted data transactions arising from the official business of the United States Government, Federal law or international agreements, drug, biological, and medical device authorizations, and other clinical trials in §§ 202.504, 202.507, 202.510, and 202.511, respectively. Section 202.504 also covers data transactions conducted pursuant to a contract, grant, or other agreement with Federal departments and agencies, even when there is concurrent funding from non-Federal sources.

At least one commenter suggested that prohibited data brokerage should be limited to circumstances in which the recipient of the data receives a right, remedy, power, privilege, or interest with respect to the data. The Department declines to make the suggested change because it fails to adequately address the national security risk posed by countries of concern or covered persons' access to government-related data and bulk U.S. sensitive personal data. The commenter's suggestion would undermine the data-brokerage prohibition and effectively give adversarial nations unfettered access to bulk U.S. sensitive personal data or government-related data. Subpart E of the regulations offer carefully tailored exemptions that balance the national security imperatives of the Order with legitimate economic and humanitarian activities, among others. Data transactions that qualify for such exemptions would not be prohibited under this program.

One commenter sought clarification or changes regarding Example 4 in § 202.214 as to whether, assuming all other requirements of the prohibition in § 202.301 were satisfied, internet Protocol (''IP'') addresses and advertising identifiers alone, without bulk precise geolocation information, would constitute prohibited data brokerage. The Department revised the example to clarify that a data transaction involving bulk quantities of U.S. users' IP addresses and advertising IDs would qualify as a prohibited data-brokerage transaction involving bulk covered personal identifiers because IP addresses and advertising IDs are listed identifiers. However, a data transaction involving only one of the listed identifiers—for example, only IP addresses—would not qualify as a covered data transaction because IP addresses in isolation do not qualify as sensitive personal data. Countries of concern may use IP addresses in some instances to aid in identifying the location of a particular device or user. However, the Department recognizes that IP addresses alone may not provide enough detailed information about a specific user or device to qualify as ''precise geolocation data.'' The Department understands that, in most commercial instances, IP addresses are collected in datasets that often contain well into the tens or hundreds of millions of such addresses and often involve other listed identifiers, as well. Given this reality, the Department will only treat IP addresses as a listed identifier, rather than also as precise geolocation data.

Another commenter recommended narrowing the definition of ''data brokerage'' primarily by striking the phrase ''similar commercial transactions'' from the definition, which the Department discussed in part IV.B.2 of this preamble. The commenter also provided some high-level examples of activities that they believe should not be considered data brokerage: (a) Marketplace sales, in which a third-party seller that is located in a country of concern or that is a covered person provides items for sale to U.S. persons on platforms owned by U.S. persons; (b) retail advertising networks that are owned by U.S. companies and that feature advertisers who are covered persons or that are based in a country of concern; (c) personal health data and human genomic data for scientific research and regulatory purposes; and (d) provisions of services to U.S. individuals abroad.

As this preamble and the NPRM explained, the Department declines to revise the definition of ''data brokerage'' because it ''is intentionally designed and scoped to address the activity of data brokerage that gives rise to the national risk, regardless of the entity that engages in it'' [and] intentionally regulates data transactions'' that give rise to the risks the Order was intended to mitigate.[65] The commenter did not address how or whether their recommended approach to data brokerage would mitigate such risk. In addition, the rule already accounts for the examples provided by the commenter. Transactions ordinarily incident to the provision of covered personal identifiers and personal financial data as part of e-commerce (such as marketplace sales) are generally exempt under the financial services exemption. With respect to scientific research and regulatory purposes, the rule does not prohibit research in a country of concern or research partnerships with a covered person that do not otherwise involve a covered data transaction. And the exemptions in §§ 202.510 and 202.511 already exempt certain data transactions arising from clinical trials and regulatory approvals in the context of drug, biological, and medical device authorizations. The commenter failed to provide sufficient specificity for the Department to address the other examples they provided. The recommended change, therefore, appears unnecessary at this time.

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 the comments received on those key terms and related terms in detail in the following discussion.

3. Section 202.201—Access

The proposed rule defined ''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 requested that, to ensure that compliance mechanisms do not impede legitimate research activities, the Department distinguish data access and data export. The commenter interpreted ''access'' to data as physically obtaining data, or as being able to analyze the data in a remote analysis environment where the data remains protected and cannot be exported. To this end, the commenter recommended addressing security concerns, while maintaining legitimate users' access to research data, by requiring data accessor attestation or by leveraging trusted research environments that adopt modern data protection methods and multi-layer security protocols.

The Department declines to distinguish access from export. In the national security context, the Department views both access to government-related data and bulk U.S. sensitive personal data by a country of concern or covered person as synonymous with the export of such data to the same. Further, it is unclear to the Department whether something like a ''data accessor attestation'' would be sufficient to dissuade or prevent a country of concern's intelligence or security service from seeking to access sensitive data that may be contained in a secure research environment. The Department does not believe that these types of measures on their own mitigate the counterintelligence and other national security risks identified by the Order and parts II–IV of this preamble. However, these types of measures could be one part of a broader risk-based compliance program implemented pursuant to the rule's requirements. Finally, it does not appear that such a change is necessary to minimize any impact on scientific and research activities, as the rule does not preclude research in a country of concern, or research collaborations or partnerships with covered persons, that do not involve any payment or other consideration as part of a covered data transaction.

Another commenter suggested a technical correction in the final rule to avoid inadvertently causing restricted transactions that comply with the security requirements to no longer be considered covered data transactions. The Department appreciates this clarification, which it has adopted in the definition of ''access.''

The final rule otherwise adopts the definition proposed in the NPRM without change.

4. Section 202.249—Sensitive Personal Data

The NPRM defined 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. As explained in part IV.B.16 of this preamble, the Department has changed the reference to human genomic data to human 'omic data in the final rule.

One commenter requested that the Department confirm that physical and digital dental health data records are included within the scope of sensitive personal data. The commenter pointed out that unauthorized access to dental health data poses significant security risks, as they contain not only personal health information but also can serve as a unique forensic identifier. The Department agrees and confirms that physical and digital dental health records would generally fall within the existing definition of ''personal health data'' within the scope of sensitive personal data. Section 202.241 of the rule provides an inclusive definition for personal health data that encompasses information related 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, for example, basic physical measurements and health attributes, 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 of prescribed medications. The data contained in

[65] 89 FR 86131.

dental records would generally relate to the past, present, or future physical health or condition of an individual and to the provision of healthcare to an individual, which the Department intentionally scoped broadly to avoid the risk of inadvertently omitting relevant health data types. This flexibility allows for new health-related fields or data types to be included in the future without needing to update the rule. Further, to the extent that any such dental health records constituted ''measurable physical characteristics or behaviors used to recognize or verify the identity of an individual,'' the definition of ''biometric identifier'' included in ''sensitive personal data'' would capture those records. In light of the Department's confirmation and the existing definition, the Department does not believe it is necessary to adjust the inclusive definition of ''personal health data'' to refer to one specific type of personal health data.

One commenter questioned the inclusion of human genomic data as a category of sensitive personal data, arguing against the ability to identify individuals solely through genetic testing and arguing that the NPRM overstates the predictability of human genomic data. The commenter agreed that knowledge of a person's genome may offer insights into potential risks and tendencies, but the commenter concluded, without citing any reference materials, that such data cannot accurately predict health, emotional stability, or mental capacity for most individuals. The commenter also suggested that it would be ''impractical'' to design genetically targeted bioweapons against a specific individual or group. As noted in the NPRM, human genomic data 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.[66] Human genomic data, even when de-identified, can still be re-identified, particularly when combined with other datasets such as medical records, health information, public databases, or social media information. This potential for re-identification highlights the necessity of the national security protections set forth in the NPRM and this preamble. The commenter's contention that a foreign adversary's government would not leverage human genomic data due to such efforts being ''impractical'' is contrary to the publicly available assessments of the United States Government, including the U.S. Intelligence Community.[67] For this and other reasons already discussed in the NPRM,[68] the Department declines to adopt any change in response to this comment.

The proposed rule categorically excluded 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. As discussed in further detail in part IV.B.15 of this preamble, the Department has refined the definition of ''sensitive personal data'' to ensure that the exclusion for publicly available data applies to each subcategory of sensitive personal data, and thus also applies to the term government-related data. In addition, as discussed in part IV.D.1 of this preamble, the Department has extended the exclusions to include certain metadata related to expressive information and informational materials.

As noted in the NPRM, nothing in the final rule shall be construed to affect the obligations of United States 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.[69] The NPRM defined two subcategories of covered personal identifiers: (1) listed identifiers in combination with any other listed identifier; and (2) listed identifiers 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. The definition included 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.

Multiple commenters requested that the Department clarify the applicability of the demographic data exclusion with respect to data brokerage. The Department directs the commenters to the definition of ''covered personal identifier'' in § 202.212(b), which excludes ''[d]emographic or contact data that is linked only to other demographic or contact data.'' That definition, in combination with the examples provided, demonstrates how demographic data and data brokerage interact with one another. Example 3 in § 202.212(c)(3) states that 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.''

The data in this example does not satisfy the definition of ''covered personal identifiers.'' Therefore, such data would not be considered sensitive personal data under § 202.249, and a transaction involving such data would not be a covered data transaction under § 202.210. In relevant part, § 202.301 only prohibits U.S. persons from knowingly engaging in a covered data transaction involving data brokerage with a country of concern or covered person. Because there is no covered data transaction, a U.S. person would not be

[66] 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*].

[67] 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 (Feb. 2021), *https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/NCSC_China_Genomics_Fact_Sheet_2021revision20210203.pdf* [*https://perma.cc/BL4H-WJSW*].

[68] 89 FR 86156–65.

[69] 89 FR 15428–29.

prohibited from engaging in a data-brokerage transaction with a country of concern or covered person involving the data from this example.

The same commenters also recommended that the Department amend the definition of ''covered personal identifier'' to exclude combinations of what the commenters claim to be low-risk identifiers, such as when advertising or device identifiers are combined with low-risk identifiers like IP addresses or contact data but not combined with any other information. The Department addressed this in the NPRM and declines to make the recommended change here. Specifically, the Department stated in the NPRM that ''covered personal identifiers and unique IDs can be used to link other datasets containing more exploitable information.'' [70] For example, countries of concern and covered persons can use such identifiers to ''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 [Subscriber Identity Module (''SIM'')] card numbers to personal mobile devices, home addresses, and government mobile devices.'' [71] Additionally, the definition of ''covered personal identifier'' in § 202.212 already excludes demographic or contact data that is linked only to other demographic or contact data.

Several commenters took issue with the Department using a definition of ''covered personal identifier'' that is different than what is considered sensitive data under other laws. Because of this, the commenters recommended a broad exemption for any data that is processed by a covered person on behalf of a U.S. person where: (1) the purpose of the processing is product research, development, or improvement; (2) the U.S. person directs and controls the manner of processing the data; and (3) the covered person is contractually bound by the U.S. person to maintain the privacy and security of the data. At least one commenter objected to the inclusion of truncated government identification or account numbers in the definition of ''listed identifier.'' The commenters further requested an exemption for data provided or transferred by internet ecosystem providers in the ordinary course of providing internet exchange, traffic management, routing, and related services designed to optimize and secure access to services by internet end-users (except when involving data brokerage) in addition to an exemption for any combination of the following: (1) a device- or hardware-based identifier; (2) an advertising identifier; and (3) a network-based identifier.

At least one of the commenters also made these recommendations in response to the ANPRM, and the Department considered them in the NPRM. However, the commenter provided no new information for the Department to act on or consider in this instance. The rule's use of the term ''covered personal identifiers'' is much narrower than what is covered by various privacy-oriented laws and regulations. The Department has already adopted similar suggestions received from other commenters to arrive at a narrower category as described in § 202.212(a)(2) and included several examples. *See* § 202.212(c). Section 202.212(b)(2) excludes identifiers critical to the operation of services and devices ''as necessary for the provision of telecommunications, networking, or similar service.'' [72] The proposed exemption mirrors generally prevalent commercial contractual obligations between data controllers and data processors (as those terms are defined by various privacy laws). The Department declines to adopt these recommendations because these conditions are targeted at fulfilling privacy-law requirements and will not address the national security risks identified in the Order. In the absence of any new evidence or support, the Department declines to remove truncated government identification and account numbers from the definition of ''listed identifiers'' for the reasons detailed in the NPRM.[73] The Department declines to add other internet service-related exemptions, as § 202.212(b)(2) already contains the requested exclusion.

A commenter in the public research field applauded the proposed rule but suggested that Social Security numbers be classified as a covered personal identifiers. Social Security numbers are included in the definition of ''listed identifier'' in § 202.234, which in turn is incorporated into the definition of ''covered personal identifiers'' in § 202.212.

Another commenter requested that the definition of ''covered personal identifiers'' exclude data that has been anonymized, de-identified, pseudonymized, aggregated, or is otherwise considered publicly available in accordance with privacy laws. The Department declines to amend this definition. As the Department has explained in response to comments to the definitions of bulk U.S. sensitive personal data and sensitive personal data, even anonymized data, when aggregated, can be used by countries of concern and covered persons to identify individuals and to conduct malicious activities that implicate the risk to national security the Order was intended to address.

One commenter recommended ''remov[ing] network identifiers from [the] set of listed identifiers,'' or that the Department eliminate § 202.234(g) on network identifiers altogether. As the commenter noted, the Department has already carved out exceptions for network-based identifier data that is only linked to other network-based identifier data. However, when these identifiers are linked to other types of sensitive personal data, the national security risks identified in the NPRM are more likely to be present. Therefore, the Department declines to implement the commenter's recommendations.

6. Section 202.234—Listed Identifier

The proposed rule defined 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.

One commenter suggested that the Department remove the fifth category (advertising identifiers) from the definition of ''listed identifiers,'' arguing that advertising identifiers are not

[70] 89 FR 86162.

[71] *Id.*

[72] 89 FR 86206.

[73] 89 FR 86124.

personal information and that prohibiting the free flow of advertising identifiers will seriously affect the development of the internet advertising industry. The Department disagrees. As articulated in the NPRM, advertising identifiers combined with other types of covered personal identifiers are indeed linked or linkable to an individual and therefore are included in the scope of bulk U.S. sensitive personal data.

One commenter recommended that the Department remove any reference to IP addresses from the rule due to the potential for businesses to refrain from or be hindered in providing communications and cybersecurity services. The commenter asserted that the NPRM referenced IP addresses in multiple ways that deviate from their normal use. Specifically, the commenter highlighted that IP addresses are sometimes associated with more than one individual, and that one individual may use multiple IP addresses depending on their location (at home, on their mobile device, at work, etc.).

Further, the commenter identified alternative identifiers such as call detail data and contact data that are frequently used with IP addresses, suggesting that including IP addresses is redundant. Finally, the commenter notes the challenges that entities have had in complying with foreign laws that regulate IP addresses as personal data and suggested that regulating IP addresses in this rule will further strain those entities.

The Department notes that the definition of ''covered personal identifiers'' in § 202.212(b)(2) excludes 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. The Department disagrees that the inclusion of IP addresses is unnecessary and should be removed from the rule. IP addresses are capable of being linked or linkable to a U.S. person and can provide location data (including, in some circumstances, precise geolocation data). The fact that IP addresses are sometimes shared or could be attributed to more than one person in some circumstances does not preclude them from also being capable of identifying U.S. persons. To the contrary, even when they can be attributed to more than one person in some circumstances, IP addresses can be useful in narrowing down, and thus increasing the identifiability of, other data that is linked or linkable to a U.S. person. As the NPRM explained, location data that can be derived from an IP address can provide important information related to patterns of life, such as when a person goes from home to work and other locations.

Finally, the rule already separately exempts (1) from the definition of covered personal identifiers, network-based identifiers, call-detail data, or account-authentication data that is linked only to other network-based identifiers, call-detail data, or account-authentication data; (2) from the prohibitions and restrictions, any transaction that is ordinarily incident to the provision of telecommunications services; and (3) from the prohibitions and restrictions, personal communications. The comment did not identify what specific non-exempt transactions with countries of concern or covered persons remain that would be prohibited or restricted, nor did it explain how those transactions are integral to the delivery of communications or cybersecurity services. No change to the rule appears necessary.

7. Section 202.242—Precise Geolocation Data

The proposed rule defined ''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. Two commenters suggested that the Department narrow the geographic radius of precise geolocation data to align with U.S. State privacy laws. No change was made in response to these comments. As a threshold matter, the rule is already consistent with privacy laws when accounting for available options on most devices. Specifically, the California Privacy Rights Act, which a few commenters cited as the standard the Department should follow, includes a geographic radius of 1,850 feet (approximately 563 meters).[74] As indicated in the NPRM, the Department 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. Furthermore, as the NPRM explained, the Department also examined Android and iOS software developers' available settings for the precision of geolocation readings, which included accuracy to within 10 meters, 100 meters, 1,000 meters, 3,000 meters, and 10,000+ meters.[75] As discussed in the NPRM, the Department concluded that location data at a distance greater than 100 meters was still considered precise and presented an unacceptable risk to national security, so 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.

One commenter suggested lowering the geographical location range from 1,000 meters to 100 meters, arguing that the proposed range was too wide and may include many civil facilities, such as enterprises, factories, and houses. The Department believes geolocation data within a distance of 1,000 meters to be precise. For example, in guidance to its members, the Network Advertising Initiative,[76] a non-profit trade group that crafts policies that protect users' privacy in the advertising technology and digital advertising space, stated, ''If a member receives information locating a user or device to an area with a size of 1,000 [square] meters, that member can render the data imprecise by only storing information that the user or device was in an area with a size of 800,000 meters.'' [77] Further to the point, this comment seems to confuse the government-related geolocation data list in § 202.1401, with the distance of precise geolocation data for the other regulated covered data transactions in § 202.242. The Department declines to adopt the recommendation.

The definition of ''sensitive personal data'' excludes public or nonpublic data that does not relate to an individual. Two commenters requested clarity on the meaning of the exclusion ''does not relate to an individual'' from sensitive personal data in the context of precise geolocation data. In particular, the commenters sought a definition of what ''relate to an individual'' means or a clarifying example to explain what relates to an individual means when precise geolocation data is defined

[74] *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).

[75] *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*].

[76] Network Advert. Initiative, *About the NAI, https://thenai.org/about-the-nai2/* [*https://perma.cc/GFN4-DVZ3*] (showing that the Network Advertising Initiative (NAI) is a non-profit, self-regulatory association dedicated to responsible data collection and its use for digital advertising).

[77] Network Advert. Initiative, *Guidance for NAI Members: Determining Whether Location is Imprecise* 3 (Feb. 2020), *https://thenai.org/wp-content/uploads/2021/07/nai_imprecise location2.pdf* [*https://perma.cc/U7CS-YHR5*].2020).

regarding an individual or a device. They note that precise geolocation data is defined in terms of U.S. devices, and therefore precise geolocation data that is de-identified should be excluded from the scope of the rule.

The Department does not believe it is necessary to create a new definition regarding ''relate to an individual.'' This phrase in the exclusionary language of § 202.249(b)(1) is intended to avoid regulation of proprietary data, trade secrets, and other data that does not have to do with individuals. Similarly, the term ''U.S. device'' is already limited to devices that ''store or transmit data that is linked or linkable to a U.S. person.'' *See* § 202.257. This definition does not capture all geolocation data that derives from a U.S. device. For example, a company may use U.S. devices to track the geolocation data of corporate assets or packages for delivery without tying that data to the individual using the device. That data would not constitute precise geolocation data because the location of corporate assets or packages does not ''relate to an individual'' and because the data is not ''linked or linkable to a U.S. person.'' If, however, the company ties the geolocation data of those assets or packages to the individual handling the U.S. device, the geolocation data would ''relate to an individual'' and would be ''linked or linkable to a U.S. person.'' Of course, how the U.S. company collects and handles that data in the United States would not be regulated by the rule; only non-exempt transactions that are prohibited or restricted involving that precise geolocation data would be regulated under the rule.

8. Section 202.204—Biometric Identifiers

The proposed rule defined ''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.

One commenter raised concerns that the proposed definition is broader than the current understanding of the term and claimed it could include photos or pictures. The commenter suggested that the Department narrow the definition of ''biometric identifiers'' to only include data that relates to personal characteristics, has been processed using specific technologies, and can uniquely identify a person. The commenter asserted, without support, that this definition is closer to the traditional understanding of the term and would therefore align with existing compliance activities.

The Department declines to adopt this recommendation. The definition of ''biometric identifiers'' already includes similar limitations; biometric identifiers are defined as ''measurable physical characteristics or behaviors used to recognize or verify the identity of an individual.'' *See* § 202.204. Further, adding a technological processing component to the definition prevents any kind of raw data from meeting the definition of a biometric identifier, allowing countries of concern to acquire biometric identifiers and then conduct the technological processing themselves. Limiting the definition to data processed using specific technologies would also risk allowing new technological developments to undermine the definition. The Department believes this definition is effectively scoped to the national security risk, and declines to narrow the definition, particularly based on unsubstantiated compliance benefits. Finally, the rule already separately excludes expressive information or informational materials from all of the categories of sensitive personal data (including biometric identifiers), so it appears unnecessary and redundant to adjust this specific definition to address the commenter's concern. Therefore, the Department makes no change to the definition of ''biometric identifiers'' in the final rule.

9. Section 202.224—Human 'Omic Data

The proposed rule sought comment on the effect of regulating human genomic data and whether to regulate other categories of human 'omic data. Several commenters expressed concerns about regulating covered data transactions involving human genomic data. For example, some commenters opposed setting the same bulk threshold for human genomic data that involves the ''entire set . . . of the genetic instructions found in a human cell'' and data that involves a ''subset'' of such instructions, as the rule defines ''human genomic data.'' *See* § 202.224(a)(1). Commenters explained that there is a low risk of identifying a single individual from a subset of genetic instructions, incomplete human genomes, or data about single genes that do not reveal information that is consequential to the health of a U.S. person or particular U.S. populations. The Department declines to change the threshold for human genomic data. As described in the NPRM, countries of concern, including the PRC, ''view . . . genomic data as a strategic commodity to be collected and used for its economic and national security priorities.'' [78] As the NPRM explains, this data poses risks not only for ''identifying traits such as health, emotional stability, mental capacity, appearance, and physical abilities that might be useful in intelligence recruitment,'' but also because ''countries of concern may also use this data to develop military capabilities such as bioweapons.'' [79] The Department declines to raise the bulk threshold applied to bulk human genomic data because the national security risks posed by country of concern access to such data include risks unrelated to a country of concern's ability to identify particular individuals or U.S. populations from such data.

Other commenters questioned the necessity of the rule, arguing that current research practices already handle genetic data securely with strong privacy considerations, such as de-identification and pseudonymization. As the NPRM explains, however, ''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,'' allowing them to ''reveal exploitable sensitive personal information on U.S. persons.'' [80] Accordingly, the Department declines to exempt from its prohibitions and restrictions human genomic data that has been de-identified or pseudonymized, outside the exemptions permitted by §§ 202.510 and 202.511, which are subject to additional oversight by the Federal Government or support data sharing necessary for regulated parties to obtain or maintain regulatory approval or authorization to market or research drugs or other products. In addition, some commenters expressed concerns that the rule could impose unwanted administrative burdens on U.S. researchers by creating roadblocks to data sharing, thereby potentially decreasing the global competitiveness of U.S. genetics research. The Department has calibrated the rule to balance the interests in maintaining U.S. competitiveness in science and research with the pressing national security risks identified by the Order and in this rulemaking. The Department has adopted, clarified, and revised exemptions in part IV.E of this preamble to help alleviate the burden on

[78] 89 FR 86142.

[79] 89 FR 86157.

[80] 89 FR 86126.

individuals conducting human genomic-related research.

One commenter noted the risk that policy makers and the media could portray human genetic data as exceptional and dangerous, which could erode public trust in scientists and negatively impact recruitment for research studies. The Department appreciates the commenter's concern but notes that the U.S. intelligence community has identified specific national security risks posed by country of concern access to bulk U.S. human genomic data that the rule seeks to mitigate and that outweigh the speculative and indirect risks to public trust in scientists asserted by the commenter.[81] Finally, the commenter contended that it is difficult to identify individuals solely through genetic testing, arguing that the predictability of human genomic data is overstated in the NPRM. As described elsewhere in part IV.B.9 of this preamble, country of concern access to bulk human genomic data poses national security risks beyond identifying discrete individuals or populations that the rule's restrictions and prohibitions are intended to mitigate.

In the NPRM, the Department sought comments about whether and how it should regulate transactions involving access to bulk human 'omic data other than human genomic data. The Department received several comments on this topic, including one that supported robust regulation and others that either opposed including other human 'omic data in the rule or proposed delaying its inclusion to a separate rulemaking. After further consideration, the Department has determined in the final rule to treat three categories of other human 'omic data—epigenomic data, proteomic data, and transcriptomic data—similarly to its treatment of human genomic data. The bulk threshold for these additional categories of human 'omic data will be higher than for human genomic data. The Department is not including any other categories of human 'omic data in the rule at this time. The Department incorporates this change by defining a new term, ''human 'omic data,'' that includes human genomic data and each of the three listed other human 'omic categories.

At a high level, the 'omics sciences examine biological processes that contribute to the form and function of cells and tissues.[82] Many commenters urged the Department to move cautiously in regulating other human 'omic data to avoid disrupting the development of new and promising fields of research. Although none of these comments spoke with any specificity about the risks of regulating covered data transactions as contemplated by the NPRM, the Department agrees that a cautious approach is needed.

The Department recognizes that not all categories of human 'omics data present the same degree of risk if accessed by a country of concern or covered person. Data from some human 'omic categories, for example, do not present the same identifiability concerns that exist for human genomic data. But the Department remains deeply concerned by the national security risk associated with transactions involving human epigenomic, proteomic, or transcriptomic data. The fields of epigenomics, proteomics, and transcriptomics are—after genomics—the most advanced 'omic fields.[83] Generally speaking, epigenomics is the study of changes in gene expression that do not involve alterations to the DNA sequence itself. The field of proteomics generally aims to identify and characterize proteins and study their structures, functions, interactions, and post-translational modifications. The field of transcriptomics generally aims to understand gene expression patterns, alternative splicing, and regulation of RNA molecules. These three human 'omic categories have the greatest clinical and predictive capacity, especially when used in combination with genomics and other 'omic categories, because they are most closely related to genomics.

Data in these categories may be used by countries of concern in numerous ways. This includes risk related to identifiability, particularly for human transcriptomic data, but also, as one commenter indicated, for human epigenomic data, human proteomic data, and human meta-multiomic data.[84] But the risks are not limited to identifiability, and countries of concern might leverage access to bulk U.S. human 'omic data in other ways that are adverse to U.S. national interests. The same attributes that make this data useful for general research make it potentially useful for nefarious purposes—for example, to train AI systems enabling the military capabilities of adversaries and undermining the U.S. bioeconomy. Additionally, classified reporting reviewed by the Department further underscores the risks of allowing countries of concern to access U.S. person data in these categories.

In addition to the comments, the Department has also reviewed a November 2024 limited study performed by the Science and Technology Policy Institute (''STPI'') that sought to preliminarily evaluate the effect on ongoing or planned research if the Department regulated human genomic and other human 'omic data in this rulemaking.[85] That study, which used various methods to estimate the effect of the contemplated regulations on research efforts (including surveying and interviewing potentially impacted stakeholders), concluded that there was unlikely to be substantial disruption to research. The report, though limited by its scope and methodology, concluded that only ''a small proportion of the U.S. research community is participating in research that involves collaboration with a country of concern'' and that even ''among groups that do have existing research collaborations with a country of concern, none of those collaborations involved data sharing that would constitute a transaction of bulk human 'omic data.'' [86] STPI's review of clinical trials identified only a single clinical trial that is currently active in the United States, involves more than 100 participants, gathers 'omic (in this case, transcriptomic and genomic) data, and has a site in China.[87]

Most of the concerns identified in the STPI report arose from general compliance concerns, such as that Federal funding entities would impose different requirements or that researchers would have to adjust computer security protocols. For example, one interviewee noted that it took substantially longer to build infrastructure to facilitate data sharing when cybersecurity requirements had to be met.[87] Another thought that research would be slowed because of confusion

[81] *See, e.g.,* 89 FR 86142, 86178.

[82] *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*].

[83] Carly S. Cox et al., *Information Gathered on the Potential Impact of Including Omic Data in a Rule on Access to Sensitive U.S. Data,* Appendix A (Science and Technology Policy Institute, Nov. 2024) [hereinafter *STPI Report*] (citing Dai and Shen 2022). The full STPI Report is available on *regulations.gov* (Docket No. NSD–104).

[84] *See, e.g.,* Patrycja Daca-Roszak & Ewa Zietkiewicz, *Transcriptome Variation in Human Populations and Its Potential Application in Forensics,* 60 J. Appl. Genet. 319 (Nov. 2019), *https://doi.org/10.1007/s13353-019-00510-1.*

[85] *See* STPI Report, *supra* note 83.

[86] *Id.* at 38.

[87] *Id.* at 40. The report found generally low levels of clinical trials of any sort that also involved a site in a country of concern.

about the scope of the rule during implementation.[88] One interviewee observed that the institutional burden of complying with new rules would limit collaboration with researchers in countries of concern.[89] It is hard to disentangle these concerns from the other provisions of the rule, and it is likely that also regulating these three categories of other human 'omic data will pose only limited marginal costs to research and industry compared to the costs attributable to other aspects of the rule, including the provisions pertaining to human genomic data. Indeed, one interviewee expressly predicted that including other human 'omic data in the scope of the regulation would have no change on the regulatory burden because 'omic research almost always also involves genomic data.[90]

Given the significant national security risks posed by country of concern or covered person access to these data, the limited available evidence to characterize the marginal disruptive effect of regulating these human 'omics categories, and the immaturity of research and commercialization of these human 'omics and related applications at present, the Department has determined to regulate these three categories of human 'omic data.

One commenter expressed support for the inclusion of provisions regulating other human 'omic data, noting that these restrictions will significantly bolster U.S. biodefense and biosecurity. The commenter noted that bulk human 'omics data should be viewed as providing insight into how the body is affected by changes in the environment and diet, by infectious and non-communicable diseases, or by other circumstances. The commenter encouraged the Department to implement regulations restricting the transfer of human 'omic data, noting that if the United States is concerned about an outside entity using human genomic data to maliciously attack the American public via biological threats, then the information gathered via other human 'omic data—especially proteomics and metabolomics—should be considered equally and perhaps more sensitive. The Department appreciates this comment. For the current rulemaking, however, the Department has chosen to focus on the most acute threats related to human 'omic data. The Department may revisit regulating transactions involving additional human 'omic data in future rulemaking.

One comment offered specific and helpful suggestions for revising the Department's proposed definitions. The Department greatly appreciates this comment and has incorporated the commenter's suggestions as applicable to the three additional categories of human 'omic data in the final rule. For example, the definition of ''human proteomic data'' now expressly excludes routine clinical measurements. The Department made similar changes to the definitions of ''human epigenomic data'' and ''human transcriptomic data.'' The final rule also clarifies that human proteomic, human epigenomic, and human transcriptomic data include only data derived from a systems-level analysis.

In the NPRM, the Department indicated it was considering carving out pathogen data in 'omic datasets. One commenter strongly supported this exclusion, explaining that pathogen-related data serves important and unique public health functions. In the preamble to the NPRM, the Department explained that it would take a similar approach to that which the commenter suggested with respect to human genomic data; in the final rule the Department expressly excludes from the definition of ''human 'omic data'' pathogen-specific data embedded in 'omic data sets.

Another commenter stressed that, if the Department includes other human 'omic data, it must also include them in the exemptions in subpart E, including for regulatory approval data and clinical investigations in §§ 202.510 and 202.511. The Department agrees. Those provisions already exempt transactions within their scope from the provisions in subparts B and C, which are the operative provisions prohibiting or restricting transactions. Application of those exemptions does not turn on the type of data involved, and the exemptions apply equally to transactions involving human 'omic data as to other categories of sensitive personal data.

Numerous commenters stressed that bulk thresholds for the other human 'omic categories identified in the NPRM should vary with risk and should be higher than the threshold for human genomic data. Commenters did not provide specific input on what those thresholds should be or which 'omics categories should have relatively higher or lower thresholds (except that phenomics probably presented a lower risk). The three additional 'omic categories the Department is regulating are those with the greatest national security risks at this time, but the Department agrees that, given the nascency of these fields and the relatively greater difficulty of using these 'omic data for identification, the bulk thresholds for these categories should be higher than for human genomic data. Some stakeholders requested simpler rules to minimize compliance costs, and the Department recognizes that, independent of individual risk analysis, there is a benefit to setting the thresholds for all human 'omics categories at the same level. But, in many use cases, this type of data is used together with genomic data, and so there may be limited practical effects to setting different thresholds for these human 'omics categories.[88] For these reasons, the Department uses a threshold of 1,000 U.S. persons for all these three additional categories of human 'omic data (epigenomic, proteomic, and transcriptomic data), while maintaining the 100 U.S. person threshold for human genomic data set out in the NPRM.

10. Section 202.240—Personal Financial Data

The proposed rule defined ''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 on whether ''personal financial history'' pertains solely to transactions with financial institutions or includes all purchase and payment history. The Department interprets this question as asking about the scope of the term personal financial data. The Department confirms that personal financial data in § 202.240, including payment history, applies across the board. It is not limited to purchases and payment history collected only by financial institutions.

Another commenter suggested that the Department clarify that personal financial data only includes information from sources like banks or credit statements, and not from vendors, merchants, search engines, or e-commerce records. The Department declines to adopt the recommendation. While such records are not automatically considered personal financial data, any record that contains ''data about an individual's credit, charge, or debit card, bank account, including purchases and payment history, and data in a bank, credit, or other financial statement, or in a credit report or consumer report'' meets the definition. *See* § 202.240. The same commenter suggested that personal

[88] *See, e.g.,* STPI Report, *supra* note 83, at 17.

financial data should only be restricted when it comes directly from an individual's bank accounts. However, the focus of the definition in the final rule is on the content of the records, documents, or information containing personal financial data, not necessarily the source. As the proposed rule explained, countries of concern and covered persons seek such personal financial data from any source and can combine it with other data to create vulnerabilities that malicious actors might exploit, posing national security risks.[89] Therefore, the Department declines to limit the definition based on the data source.

11. Section 202.241—Personal Health Data

The proposed rule defined ''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.

One commenter suggested that the Department remove ''or the past, present, or future payment for the provision of healthcare to an individual,'' ''social, psychological, behavioral,'' and ''logs of exercise habits'' from the definition of ''personal health information.'' This commenter argued that medical expenditures are helpful to the construction and communication of medical treatment systems but cannot directly reflect someone's disease diagnosis and treatment, and thus should not be restricted. The same commenter also asserted, without explanation, that social, psychological, behavioral and sports habits are too broad to pose any threat to national security. The Department declines to adopt the recommendation. Medical expenditures can be revealing about the nature of a diagnosis or medical issue. For example, medical billing statements often come with diagnostic codes to show the services provided by a medical practitioner or facility. An expenditure in a specific location (*e.g.,* an oncology office, obstetrics office, or dialysis center) can similarly reveal information about health conditions. Likewise, data such as social, psychological, or behavioral habits on a specific individual can be exploited by a country of concern as a means of recruitment by an intelligence service (particularly via blackmail or coercion). This data in the hands of a country of concern could certainly pose a risk to U.S. national security, as shown by numerous open-source examples in this preamble and the NPRM's preamble in which reporters and researchers used precisely this kind of data (such as exercise logs) to track, surveil, and glean insights on U.S. military activities and personnel overseas. The rule thus adopts the approach described in the NPRM without change.

As the NPRM described, this proposed definition operates on a categorical basis and determines 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 ''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. The Department welcomed comment on the extent to which there is discrete data related to an individual's physical or mental health condition that is not inherently linked or linkable to U.S. individuals (such as a dataset of only heights or weights with no identifying information).

Commenters did not address the Department's question. Instead, several commenters raised issues with the Department's use of the term ''relates'' in the proposed rule's definition of ''personal health data.'' The commenters urged the Department to define the term, or to narrow the definition of ''personal health data'' to replace the term ''relates'' with other terms, such as ''identifies'' or ''reveals.'' They contended that data that ''relates'' to an individual, but does not identify an individual, has a low potential to cause harm but is essential to commerce, access to goods and services, and to ensuring that innovation is not stifled. One commenter mentioned that the term ''relates'' is so broad that it could apply to the sale not only of a prescription, but also to innocuous retail purchases that relate to a condition but do not identify it, such as the purchase of tissues at a supermarket.

The Department has revised the definition of ''personal health data'' to provide greater clarity, particularly for regulated parties not typically governed by the Health Insurance Portability and Accountability Act of 1996 (''HIPAA'') or familiar with its terminology. Personal health data within the rule's scope must *indicate, reveal, or describe* the past, present, or future physical or mental health 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.

However, the Department declines to replace the term ''relates'' with the term ''identifies.'' The commenters do not support their assertion that data that does not identify individuals on its face has a low potential to cause harm. The rule intentionally does not define personal health information in terms of whether the information identifies individuals, because the rule applies across the board, regardless of whether data is de-identified. This approach responds to the national security risks posed by countries of concern that may have the ability to re-identify the data. The Department discussed these risks in detail in the NPRM, and in part IV.B.4 of this preamble. The Department also notes that the definition of ''personal health data'' includes an illustrative list of the types of data that the term includes, including the use or purchase of prescribed medications. Although this list is not exhaustive, it demonstrates the kinds of personal health information that the Department intends the definition to cover.

One commenter contended that the HIPAA de-identification standards are out of date, and do not protect individuals in today's data-rich and computational-rich environment. The commenter commended the NPRM for addressing the ever-increasing ability to re-identify supposedly de-identified data, requested that traditional de-identified HIPAA data be subject to the final rule, and further proposed that de-identified personal health data such as medical records, pharmacy records, and reproductive health records or purchases be covered by the final rule. The Department agrees with this recommendation.

One commenter agreed with the need to regulate personal health data and suggested that the Department discuss the regulations with electronic medical record organizations and hospital associations. The Department, both on its own and with other agencies, discussed the NPRM with 44 medical organizations, associations, and other stakeholders that will be impacted by the regulations, comprised of healthcare trade associations, biotechnology

[89] *See, e.g.,* 89 FR 86161.

organizations, research laboratories, and universities.

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

The prohibitions and restrictions apply to ''bulk U.S. sensitive personal data,'' which the proposed rule described 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.

Three commenters mistakenly noted that the definition of ''bulk U.S. sensitive personal data'' did not include a definition for ''sensitive personal data'' or ''sensitivity'' and could, as a result, be interpreted too broadly to cover all data, not just sensitive data. As shown in the ANPRM and NPRM, the proposed rule already incorporated a separate definition of the term ''sensitive personal data'' in § 202.249, which is limited to the six categories of bulk U.S. sensitive personal data. Furthermore, the definition of ''bulk,'' as provided in § 202.205, incorporates this definition of ''sensitive personal data.'' Therefore, the term ''bulk U.S. sensitive personal data'' is appropriately scoped. However, another commenter recommended that the Department amend the definition of ''bulk U.S. sensitive personal data,'' which says, ''a collection or set of bulk data,'' to align with the characterization of the term in the part IV.A.13 of the NPRM, which says ''a collection or set of sensitive personal data.'' The Department agrees and has updated the definition of ''bulk U.S. sensitive personal data'' accordingly to ensure consistency, which should help further clarify the scope of bulk U.S. sensitive personal data. The Department has amended the definition of ''bulk U.S. sensitive personal data'' to read as follows: ''The term *bulk U.S. sensitive personal data* means a collection or set of sensitive personal data relating to U.S. persons, in any format, regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted, where such data meets or exceeds the applicable threshold set forth in § 202.205.''

One commenter asked for clarification on whether precise geolocation data and personal health data include de-identified data. The Department encourages this commenter to review § 202.206. Three commenters suggested that the Department include definitions for the terms ''anonymized,'' ''pseudonymized,'' and/or ''de-identified.'' One such commenter recommended, in the context of the exemptions listed in §§ 202.510 and 202.511, that the Department adopt a definition of ''de-identified'' that is consistent with the privacy protection standards required by the U.S. Food and Drug Administration (''FDA'') as part of post-marketing adverse event reporting; namely, that the data be coded and not include individual names or addresses. The Department declines to adopt this suggestion. Such techniques evolve over time, and the final rule is intended to capture these developments and remain technology neutral. As one of the above commenters admitted, these are terms that are not universally understood to mean the same things. More broadly, these terms in the definition are meant to capture any claimed method for or attempt at anonymizing, pseudonymizing, or de-identifying sensitive personal data. As explained below in this part of the preamble, by including any attempt at anonymizing, pseudonymizing, or de-identifying sensitive personal data within the scope of ''sensitive personal data'' but then authorizing restricted transactions that comply with the methods of anonymization, pseudonymization, and de-identification laid out in CISA's security requirements to the extent such methods are sufficient to fully and effectively prevent access to covered data that is linked or identifiable (or unencrypted or decryptable), the rule promotes effective methods while prohibiting ineffective methods. No change to this rule thus appears necessary.

Several commenters suggested that the Department modify the definition of ''bulk U.S. sensitive personal data'' to exclude data that is anonymized, pseudonymized, or de-identified ''in compliance with internationally recognized industry standards.'' These commenters suggested that such an approach would be appropriate where the link between the identifying dataset and the individual has been removed, where the data has been de-identified pursuant to HIPAA ''expert determination'' de-identification methods, or where the data has been ''reasonably deidentified where a data controller has taken a clearly defined risk-based approach.'' Many of these commenters argued that it is difficult to tie anonymous or de-identified personal information to an individual or an individual's device and that such information is therefore not sensitive personal data. One commenter noted that effective de-identification, consistent with clear standards, has proven protective of individual privacy interests and is critical for research that leads to medical advancements. Another commenter argued that the Department's cited studies did not offer definitive evidence that re-identification of truly anonymized data is a real risk, but the commenter provided no evidence to contradict the cited studies or to support their conclusion. Another commenter said that control measures for anonymized, pseudonymized, and de-identified data should be different than control measures for unprocessed original data. Finally, one commenter noted that the Department should instead direct DHS to identify standards for de-identifying and anonymizing data that meet certain requirements.

Other commenters suggested that the definitions of government-related data also exclude data that is subject to robust encryption measures, including, but not limited to, data protected via post-quantum cryptography algorithms approved by the National Institute of Standards and Technology (''NIST'') to withstand quantum computer attacks. A few commenters opposed the inclusion of encrypted data based on the proposed CISA security requirements relating to data minimization and data masking strategies for restricted transactions. One commenter noted that the inclusion of encrypted data does not represent a carefully calibrated action and would curtail the usefulness of privacy-enhancing technologies (even though some of these were explicitly included in the proposed CISA security requirements). This same commenter stated, without providing any support, that quantum-computing capabilities that could be used to decipher encrypted data are too far from being operational to decrypt bulk data. Another commenter noted that adopting an exemption for these algorithms would incentivize better encryption and promote post-quantum cryptography adoption.

The Department declines to alter the approach in the NPRM. These comments inaccurately suggest that this rule would treat anonymized, pseudonymized, de-identified, and encrypted data the same as unprocessed data. The rule does not prohibit all covered data transactions with countries of concern or covered persons whenever the sensitive personal data is anonymized, pseudonymized, de-identified, or encrypted. Instead, the rule includes such data within the scope of sensitive personal data and then authorizes the three categories of restricted transactions as long as they meet CISA's security requirements, which include data-level requirements that allow transactions to proceed with sufficiently effective techniques to accomplish data minimization and

masking, encryption, and/or privacy-enhancing technologies, and otherwise comply with the rule's other applicable requirements. For example, depending on the other circumstances of the restricted transaction, including the findings of the relevant internal risk assessment conducted in accordance with CISA's security requirements, the use of NIST-approved post-quantum cryptography algorithms would appear to satisfy the data-level requirement of applying comprehensive encryption techniques during transit and storage, as described in the CISA security requirements.

The rule's effect is therefore to strike a balance by allowing employment, vendor, and investment agreements with countries of concern or covered persons that use the robust anonymization, encryption, and/or other data-level requirements specified by CISA's security requirements along with organizational and system-level requirements, which are derived from the existing and commonly used security standards for securing data. At the same time, the rule does not allow transactions if they involve access by a covered person or country of concern to unprocessed sensitive personal data or insufficient anonymization, encryption, or other data-level requirements that do not meet CISA's security requirements.

This approach allows for restricted transactions to move forward, while setting a floor for the security applied to the underlying government-related data and bulk U.S. sensitive personal data in these transactions. As CISA explains, the final security requirements permit organizations to conduct restricted transactions by applying a sufficient combination of data-level techniques (such as pseudonymization, de-identification, aggregation, and/or encryption, as outlined in the security requirements) that either allow access to an appropriately mitigated version of the data or directly deny countries of concern and covered persons access to the data itself, in conjunction with implementing the organizational and system level requirements.

This approach is consistent with the NPRM's explanation that access to weakly anonymized, pseudonymized, encrypted, or de-identified data presents similar national security risks as access to the unprocessed or identifiable sensitive personal data. As the NPRM explained, countries of concern are attempting to access and exploit anonymized, pseudonymized, de-identified, and encrypted data (including to identify individuals). The NPRM also explained at length, using representative studies and open-source examples, how not all forms of anonymization, pseudonymization, de-identification, and encryption provide sufficient protection from re-identification. These comments do not address the NPRM's explanation, do not provide any contrary evidence, and merely state a desired conclusion. The NPRM's approach allows the Department to strike an appropriate balance between ensuring that restricted transactions can continue given their greater economic value and ensuring that there are robust safeguards in place to protect this data.

As a result, the rule's approach, coupled with CISA's security requirements, is designed to encourage the adoption of sufficiently effective methods of encryption, aggregation, and/or other privacy-preserving technologies. One of the data-level requirements available in the security requirements is to encrypt the data ''during transit and storage'' using comprehensive encryption, with secure management of the cryptographic key. As the security requirements explain, United States Government-approved encryption algorithms, ciphers, and protocols—including any United States Government-approved standards for quantum-resistant public-key cryptographic algorithms—are considered comprehensive encryption.

While post-quantum cryptography could be part of a sufficient combination of data-level requirements under the security requirements to allow a restricted transaction to go forward (so long as such encryption qualifies as comprehensive encryption), the Department declines to entirely exempt restricted transactions that implement a particular level of encryption. As the NPRM explained, the use of a strong cryptographic method is one tool to mitigate the risk of access to data. But as the security requirements make clear, encryption by itself is not a panacea. Encryption is not sufficient on its own to adequately mitigate the risk of access by a country of concern or covered person. Instead, even robust encryption must be accompanied by other measures to be effective in mitigating the risk of access. For example, comprehensive encryption must be accompanied by secure cryptographic key management (such as ensuring that the key is not co-located with the data and that covered persons and countries of concern do not have access to the key). Similarly, encryption must be implemented with the organizational- and system-level requirements to ensure that encryption is implemented effectively, for example, by treating the systems responsible for the storage of and access to encryption keys as being subject to organizational- and system-level controls that mitigate the risk that a covered person is able to access the keys to decrypt the data. And the use of even post-quantum cryptography does not eliminate the need to perform due diligence, audit compliance with the security requirements, and keep records. As a result, the Department declines to exempt restricted transactions merely because they use industry-standard encryption.

Finally, the rule offers a host of exemptions related to health research, including exemptions for federally funded research, certain clinical trials, and sharing of this data pursuant to international agreements such as certain pandemic surveillance agreements. The rule also authorizes the Department to issue general and specific licenses as necessary and appropriate.

13. Section 202.205—Bulk

The NPRM proposed applying the proposed rule's prohibitions and restrictions to bulk amounts of U.S. sensitive personal data (in addition to the separate category of government-related data). The proposed rule defined ''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 Department proposed volume-based thresholds for each category of sensitive personal data and for combined datasets. *See* § 202.205. 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 the ANPRM, the Department previewed ranges within which each of the bulk thresholds would be selected, relying on orders-of-magnitude differences to develop preliminary judgments.[90] The Department sought input on the thresholds from the public in response to the ANPRM. While commenters expressed varying views (including that the potential thresholds were too high or too low, should be zero, or should be eliminated entirely), these comments merely stated their preferred numbers.[91] None of the comments provided actionable data points, use cases, or evidence that would support an alternative analytical framework or support adopting one

[90] 89 FR 15786.

[91] 89 FR 86164.

particular threshold over another. Given this 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, but those engagements did not yield any materially new qualitative or quantitative information to reliably inform the selection of the bulk thresholds.[92]

In the NPRM, the Department proposed thresholds within the ranges previewed in the ANPRM and set forth the relevant analysis, including the methodology and risk-based assessment for each category of sensitive personal data.[93] As part of that analysis, the NPRM examined whether potential unintended economic impacts from the choice of specific thresholds should justify deviating from the risk-based analysis and determined that it should not be based on available information. As the NPRM explained, neither the Department nor commenters identified actionable data or analysis suggesting that the specific choice of thresholds above zero is reasonably likely to result in unintended and unanticipated downstream impacts, and thus it did not appear to make a difference whether a threshold is, for example, 100 versus 1,000. The NPRM also explained that it seems unlikely that any such data or analysis exists that would be detailed and representative enough to reasonably affect the choice of any specific thresholds above zero, and there is no known, reliable, sufficiently representative qualitative or quantitative data sufficient to conclude that a choice between potential thresholds would meaningfully affect the number of transactions subject to the regulations or the cost of compliance. As at the ANPRM stage, while commenters once again expressed varying views and stated their preferred thresholds in response to the NPRM, none of the comments provided actionable data points, use cases, or evidence that would support an alternative analytical framework or support adopting one particular threshold over another. The Department of Justice (along with the Department of Commerce) once again followed up individually with commenters on this topic to seek any additional information, but those engagements did not yield any materially new qualitative or quantitative information to reliably inform the selection of the bulk thresholds.

No commenter opposed the risk-based framework and analysis that the NPRM laid out to determine the bulk thresholds, such as by suggesting an alternative methodology. Other than bare assertions of policy preferences about the thresholds, the comments addressed only discrete issues with respect to the thresholds.

The rule therefore adopts the bulk thresholds as proposed in the NPRM. The bulk thresholds analysis in the NPRM necessarily focused on orders of magnitude and set ratios based on the relative sensitivity of the six types of sensitive personal data. On the risk side, order of magnitude is the most granular level of reliable analysis given current experience and available information. Research makes clear, for example, that a relatively small amount of sensitive personal data can be used to extrapolate insights about a population that is orders of magnitude larger. By using basic statistical inference techniques, a sample size need not exceed 10 percent in order to draw conclusions about an entire population. As discussed above in this part of the preamble, fairly small sample sizes of Americans may allow for inferences on much larger segments of the U.S. population.[94] And although the Department considered whether this risk-based setting of ratios should be altered to account for potential unintended economic impacts, there is no sufficiently granular information or analysis about the types and volumes of data involved in the categories of regulated transactions to reliably inform a choice between any particular thresholds even at the level of generality of orders of magnitude. Based on the limits of currently available information, analyzing and setting the bulk thresholds at a level more granular than orders of magnitude is too speculative to form the basis for a policy decision.

Some commenters asserted that the thresholds for human genomic data are too low and will hinder normal academic, scientific, and technological exchanges. The Department declines to change these thresholds. As articulated in the NPRM, the thresholds for human genomic data are correlated to the sensitivity of that data and the national security risk when such data is exploited by a country of concern, such as the commenter. The 2024 National Counterintelligence Strategy explains that, ''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'' and ''health care data.'' [95] ODNI has explained, for example, that China has gone to great lengths to obtain Americans' human genomic data, such as trying ''to leverage access through its relationships with Chinese companies, strategic investments in foreign companies, and by purchasing large data sets.'' [96] 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.'' [97]

Additionally, no evidence has been provided that the rule would hinder beneficial academic, scientific, and technological research in light of the examples and exemptions in the rule. As explained in parts IV.B.2 and IV.D.9 of this preamble, the rule does not prohibit or restrict U.S. research in countries of concern, or research partnerships or collaborations with countries of concern or covered persons, that do not involve a prohibited or restricted commercial transaction. The rule contains exemptions meant to preserve critical health research, including the exemptions for federally funded research, for sharing data pursuant to international agreements (including certain pandemic-related and global-health-surveillance agreements), for submissions of regulatory approval data for medical drugs, devices, and biological products, and for certain clinical-investigation data and post-marketing surveillance data. Finally, as articulated in the NPRM, the rule contemplates a process through which the Department can issue general or specific licenses as necessary and appropriate to authorize regulated activities in certain circumstances.

One commenter requested that the Department delete § 202.205(c), which sets the bulk threshold for precise geolocation data at more than 1,000 U.S. devices. As justification, the commenter argued that § 202.222's Government-Related Location Data List identifies precise geographic areas, but that § 202.205(c)'s bulk threshold on precise

[92] *Id.*

[93] 89 FR 86164–65.

[94] Sandip Sinharay, *An Overview of Statistics in Education,* in International Encyclopedia of Education (Penelope Peterson et al. eds., 3d ed. 2010).

[95] Nat'l Counterintel. & Sec. Ctr., *supra* note 6, at 13.

[96] *In Camera, Ex Parte* Classified Decl. of Casey Blackburn, Assistant Dir. of Nat'l Intel., Doc. No. 2066897 at Gov't App. 11 ¶ 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.'').

[97] *Id.* at Gov't App. 11 ¶ 33(a).

geolocation data is somehow a double limit. This comment, which is unclear, seems to confuse several different elements of the rule: the Government-Related Location Data List in § 202.1401, the 1,000-meter precision required in the definition of ''precise geolocation data'' in § 202.242, and the bulk threshold of 1,000 U.S. devices in § 202.205(c). Geographic or location data must first be precise enough (within 1,000 meters) to meet the definition of ''precise geolocation data'' in § 202.242. If it is, then the question is whether that precise geolocation data provides a location within one of the areas on the Government-Related Location Data List in § 202.1401. If so, then the data is government-related data, and the bulk threshold of 1,000 U.S. devices in § 202.205(c) does not apply. If not, then the data qualifies as bulk U.S. sensitive personal data only if it exceeds the bulk threshold of 1,000 U.S. devices in § 202.205(c). As such, the Department declines to make any change in response to this comment.

Several commenters encouraged the Department to review and adjust the bulk thresholds over time to reflect changes to technology and asked how the Department might change the thresholds in the future. One commenter sought clarification regarding the benefits of setting static thresholds for technological uses that may vary widely and change rapidly. The commenter was concerned that new discoveries, particularly from AI models, could change the United States Government's risk tolerance and justify changing the thresholds. The Department intends to monitor evolving technological developments and national security threats to ensure that the thresholds remain responsive to the risks. Changes to the bulk thresholds could be accomplished through additional rulemakings.

One commenter asserted that the proposed rule did not detail how it arrived at the different bulk thresholds, aside from assessing human and machine-centric characteristics, and that an assessment should consider the effectiveness of the thresholds. The commenter did not specify what ''effectiveness'' would mean in this context. The same commenter noted that sophisticated actors would likely find ways to circumvent any thresholds, while at the same time asserting that higher thresholds for each category would help focus regulators, reduce the impact on trade and innovation, and make the program more manageable for the Department to enforce. The commenter did not provide evidence or analysis justifying these assertions.

One commenter criticized the bulk thresholds as copying the PRC Government's approach to data restrictions and suggested eliminating them. There is no basis to analogize this rule to the PRC Government's regime. Consistent with the longstanding commitment of the United States to the trusted flow of data across borders, this rule's default is to allow data transactions except for targeted prohibitions and restrictions on engaging in certain types of commercial transactions involving sensitive personal data above the bulk thresholds where that trust is lacking. The bulk thresholds thus have the effect of exempting transactions with less data. By contrast, PRC law's default is to restrict data exports and require PRC Government review unless they fall below certain thresholds or meet certain exemptions. The superficial fact that both use a numerical threshold for entirely different purposes does not make one like the other.

One commenter sought clarification on whether the bulk thresholds apply to individual legal entities or apply in total to data accumulated across subsidiaries or affiliated companies. They further sought guidance on the timeframe for calculating and implementing the bulk thresholds. The bulk thresholds apply to each entity that engages in a covered data transaction, regardless of whether the entity has a relationship to another entity, such as a parent and one of its subsidiaries. As stated in the definition, the bulk thresholds apply to any amount of sensitive personal data that meets the thresholds and that involves the same U.S. person and same foreign person or covered person. The rule defines the term ''U.S. person'' to include certain entities and, in turn, defines the term ''entity'' as ''a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization.'' See §§ 202.256 and 202.218.

One commenter requested, without support or analysis, that the rule set the bulk threshold for personal financial data and covered personal identifiers at 1 million, and another requested that the Department set the threshold for personal financial data at 500,000. Both commenters requested that the Department remove the 12-month ''look-back'' period because, as one commenter explained, the proposed bulk threshold of 10,000 is too low and the 12-month ''look-back'' period is too long. The commenter contended that many large financial institutions that conduct transactions with personal financial data will easily exceed the proposed threshold of 10,000, and thus will incur heavy compliance burdens to review every transaction to determine whether they are restricted. Combined with the 12-month ''look back'' requirement, this commenter noted that if an entity conducts just two transactions per month related to 450 U.S.-persons' financial data over a 12-month period, it would be engaging in a restricted transaction. The Department declines to revise the bulk thresholds for covered personal identifiers and personal financial data in response to these comments. As discussed in part IV.B of this preamble, the bulk thresholds are set based on a risk-based assessment that accounts for the characteristics of the different categories of sensitive personal data that affect the data's vulnerability to exploitation by countries of concern, as well as the consequences of that exploitation. These commenters did not offer any analysis or evidence about the compliance burdens on financial institutions, nor did they explain the kinds and volume of non-exempt covered data transactions that these institutions would be engaged in (especially in light of the financial services exemption that likely covers most of those institutions' global data activities).

In addition, while these two commenters considered the impact of the thresholds only in terms of compliance burdens for a single financial institution, the Department must also consider the impact of the thresholds collectively. The Department believes that, with respect to addressing the national security risk, the thresholds should be primarily examined from the perspective of the access provided to countries of concern and covered persons across all covered data transactions, rather than from the perspective of a single U.S. person's transactions with a single foreign person. If the thresholds are higher, countries of concern will be able to obtain unrestricted access to significantly larger amounts of bulk U.S. sensitive data across thousands, and potentially tens of thousands, of transactions. For example, if 50 U.S. persons each give the same covered person access to genomic data on 99 U.S. persons—a seemingly small number—then a country of concern would be able to potentially obtain unrestricted access to genomic data on nearly 5,000 U.S. persons. And as explained above in this part, the data on those 5,000 U.S. persons could be reasonably used to identify individuals or extrapolate insights about a population that are orders of magnitude

larger by using basic statistical inference techniques.[98]

To put this into perspective, raising the bulk threshold for covered personal identifiers by one order of magnitude to 1 million U.S. persons would allow a country of concern government to buy the passport numbers and Social Security numbers of every U.S. person who lives in the city of San Francisco from a U.S. company—and buy from other U.S. companies the same data for every U.S. person in Detroit, Washington, DC, Las Vegas, Jacksonville, and so on. Similarly, raising the bulk threshold for personal health data and personal financial data by one order of magnitude to 100,000 U.S. persons would allow U.S. companies to store the treatments and test results, financial transactions, and debts and assets of every U.S. person who works for T-Mobile, Ford, Citigroup, McDonald's, and General Motors in a data center operated by a country of concern state-owned enterprise with zero security precautions to mitigate the risk of access to that data. Those examples illustrate the unacceptable national security risks that would result from significantly raising the thresholds and allowing a country of concern to readily assemble and exploit a structured set of pattern-of-life data that is representative of the American population.

For these reasons, the Department must prioritize the cumulative national security impacts of transactions across the various data categories over the compliance burdens of individual entities, especially when no meaningful evidence or analysis has been presented on the latter topic. The Department therefore adopts the proposed bulk thresholds without change.

14. Section 202.222—Government-Related Data

The proposed rule defined subcategories of government-related data for locations and personnel, and it did not propose imposing any bulk threshold requirements on transactions involving government-related data.

For the location subcategory, the NPRM proposed defining ''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 which 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 proposed rule listed specific locations on the Government-Related Location Data List, and anticipated including additional locations in the final rule. The final rule includes an expanded list of locations that meet the criteria in § 202.222(a)(1). *See* § 202.1401. These additional locations consist of commonly known Department of Defense sites, installations, such as bases, camps, posts, stations, yards, centers, or homeport facilities for any ship, ranges, and training areas in the United States and its territories. These locations are controlled by the Federal Government, as they encompass land which is federally owned or otherwise federally managed. This initial list does not necessarily represent a comprehensive collection of all locations that meet the criteria for inclusion on the Government-Related Location Data List. The Department, in consultation with other agencies, will continue to consider adding additional locations to the list, which may include, for example, U.S. embassies and consulates, certain Federal department and agency headquarters locations, and other facilities or locations that otherwise support the Federal Government's national security, defense, intelligence, law enforcement, or foreign policy missions.

For the personnel subcategory, the NPRM proposed 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.[99] The Department also sought public input on a suggestion raised by a commenter that the proposed definition remove 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. The Department did not receive any public input on this question.

One commenter sought to ensure that, similar to sensitive personal data, the definition of ''government-related data'' excludes publicly available data. The Department appreciates the need to ensure that the definitions of sensitive personal data and government-related data both exclude publicly available data, and it has revised the definition of ''sensitive personal data'' in § 202.249 to clarify that each category of sensitive personal data—including precise geolocation data, which is a key part of the government-related data definition—excludes publicly available data.

One commenter stated that the defined term ''precise geolocation data'' is unclear but did not say why. Another commenter, who was supportive of the inclusion of a publicly available list of government-related locations, recommended that the list be made available in formats that allow companies to automate and streamline compliance. Although no change is needed to the rule, the Department supports automating and streamlining compliance and intends to pursue this suggestion as part of publicly maintaining this list of latitude and longitude coordinates of the geofenced areas.

One commenter asserted that the personnel category is extremely broad, open-ended, and could apply to large sections of the U.S. population. The commenter requested that the Department set a clear and high threshold for seniority in order to only capture the most important government officials, noting that a key issue for many organizations is that they have mixed data sets containing sensitive data on government officials along with data on civilians.

The Department declines to set thresholds or revise the seniority levels for government-related data. To start, as the Department explained in the NPRM, the Department has defined the personnel subcategory based on how the U.S. person markets the data, not based 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 based merely on the presence or absence of data linked to certain government personnel in the underlying sensitive personal data. The comment therefore appears premised on a mistaken assertion about how the personnel subcategory is defined. Furthermore, because the Order sets forth the personnel categories as ''current or recent former employees or contractors, or former senior officials, of the Federal

[98] Sinharay, *supra* note 94.

[99] 89 FR 86129.

Government,'' [100] the Department does not have discretion to change them. Even if it did, the risks associated with countries of concern or covered persons obtaining government-related data are not confined to the most senior government personnel, as the NPRM discussed.[101] The risk of countries of concern and covered persons identifying and recruiting United States Government personnel, for example, are not limited to the most senior government personnel,[102] and access to sensitive personal data can facilitate the identification of individuals for this type of recruitment.

One commenter suggested several changes to the definition of ''government-related data'' in § 202.222. First, the commenter argued that the language of § 202.222(a)(1)(iii) (''Facilities or locations that otherwise support the Federal Government's national security, defense, intelligence, law enforcement, or foreign policy missions'') was too vague and impractical. Second, the commenter recommended removing ''recent former employees or contractors'' from the definition in § 202.222(a)(2), arguing that former employees and suppliers are not confidential and that the prohibition would affect the normal production and ''personal life'' of the relevant organizations. Third, the commenter suggested deleting ''military personnel who like to read'' from Example 1, as written in § 202.222(b), arguing that this description is a subjective judgment.

The Department declines to adopt these recommendations. Federal agencies have identified within the list at the end of the rule the locations that these agencies want subject to the prohibition on sale of precise geolocation data. The Government-Related Location Data List is thus designed to preserve the confidentiality of the activities, personnel, and facilities in those locations, which geolocation data in those locations could be used to reveal. ''Facilities or locations that otherwise support the Federal Government's national security, defense, intelligence, law enforcement, or foreign policy missions'' is meant to demonstrate the types of facilities included on the precise geolocation list. Regarding the inclusion of former employees and contractors, Section 7(m)(i) of the Order defines the personnel subcategory of government-related data marketed as linked or linkable ''to categories of current or recent former employees or contractors, or former senior officials, of the Federal Government.'' As such, the Department has no discretion to remove this subcategory from the scope of the rule. Further, the rule is intended to protect both current and recent former employees and contractors because former United States Government employees are still a desirable target for coercion and blackmail, based on their potential insider knowledge of United States Government facilities, operations, and other details, as well as on their potential to pick up new contract work to gain access to new data in which a foreign adversary may have interest. Finally, the language from the example is meant to demonstrate how the rule works in reality. Focusing on whether the transacting party's characterization of a dataset is subjective is irrelevant to whether the transacting party has marketed the data 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.

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

The proposed rule included 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.[103] The NPRM proposed prohibiting 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. The proposed rule also included a requirement for U.S. persons engaging in such transactions to report any known or suspected violations of the required contractual provision. This requirement would create a mechanism to provide the necessary information for the Department to investigate and take appropriate action to address any violations of the proposed rule.

A few commenters asserted that this provision imposes ambiguous requirements on U.S. persons engaging in covered data transactions. They stated that it is unclear how entities should evaluate whether foreign persons are complying with the contracts, and asked that the Department explicitly describe the due diligence requirements for U.S. entities to comply with § 202.302. Regarding the reporting requirement, one commenter asked that the Department exclude inadvertent, good faith, or de minimis violations of the contracts. Another commenter argued that the use of contractual language to prevent the onward transfer of data to countries of concern or covered persons was a significant step, but emphasized that some countries or entities might find alternative means to transfer data and recommended that the Department extensively track and monitor compliance. Another commenter asked that the Department provide standard contractual clauses that meet the Department's expectations about contractual requirements.

The Department declines to prescribe specific due diligence requirements for compliance with § 202.302, because overly prescriptive requirements will not fit the risk profile or operations of all U.S. persons. As the Department discussed in detail in the NPRM, the Department expects that U.S. persons will develop compliance programs that fit their own individualized risk profiles depending on a variety of factors. At a minimum, however, U.S. persons must conduct sufficient due diligence to be able to comply with the reporting requirements, which could include periodic reviews with foreign counterparties to ensure that they have complied with the contract. The Department anticipates issuing general compliance guidance, which may include sample contractual clauses and suggest potential ways to track and monitor compliance.

Regarding excepting de minimis, good faith, or inadvertent contract violations, without a specific example, the Department cannot envision what such violations of the requirement would be. Specifically, § 202.302 requires that a U.S. person report when a foreign person has engaged in a covered data transaction—that is, a transaction that involves access by a country of concern or covered person to any government-related data or bulk U.S. sensitive personal data. Any violation of this contractual term gives a country of concern or covered person access to

[100] 89 FR 15429.

[101] *See, e.g.,* 89 FR 86118.

[102] Press Release, U.S. Dep't of Just., *Former CIA Officer Sentenced to 10 Years in Prison for Conspiracy to Commit Espionage* (Sept. 11, 2024), *https://www.justice.gov/opa/pr/former-cia-officer-sentenced-10-years-prison-conspiracy-commit-espionage* [*https://perma.cc/F9UG-AANZ*]; Press Release, U.S. Dep't of Just., *U.S. Army Intel. Analyst Pleads Guilty to Charges of Conspiracy to Obtain and Disclose National Defense Information, Export Control Violations and Bribery* (Aug. 13, 2024), *https://www.justice.gov/opa/pr/us-army-intelligence-analyst-pleads-guilty-charges-conspiracy-obtain-and-disclose-national* [*https://perma.cc/8MGA-7FWS*].

[103] 89 FR 86130.

sensitive personal data and is inherently not de minimis. Moreover, the reporting requirement does not require that U.S. persons report contractual violations unrelated to this provision, such as a foreign person missing a reporting requirement by a few days or other minor contractual provisions. Because of the nature of national security risks, even good-faith or inadvertent violations of the contractual provision may still result in harm to U.S. national security by enabling access by a country of concern or covered person to government-related data or bulk U.S. sensitive personal data through data brokerage. For those reasons, the Department declines to modify the reporting requirement to account for de minimis, good faith, or inadvertent contract violations.

One commenter suggested that the provision apply only when a U.S. person has actual knowledge that a foreign counterparty is repeatedly violating contractual provisions. Another commenter asked that the Department include the word ''knowingly'' before the term ''engaging'' (although the term already exists there), and another asked that the Department define the terms ''known or suspected [violations]'' and clarify the extent to which a U.S. person must know about a violation for the reporting requirement to be triggered.

The rule's knowledge standard is addressed in detail in part IV.B.19 of this preamble. Section 202.230 defines ''knowingly'' to mean, with respect to conduct, circumstances, or a result, that the U.S. person had actual knowledge of, or reasonably should have known about, the conduct, circumstances, or result. To determine what an individual or entity reasonably should have known in the context of prohibited transactions, the Department will consider relevant facts and circumstances, including the sophistication of the individual or entity, the scale and sensitivity of the data involved, and the extent to which the parties to the transaction appeared to be aware. The Department declines to adopt an actual knowledge standard because the knowingly standard acknowledges the doctrine of willful blindness, a legal concept where a person intentionally avoids knowing about something illegal or wrong, even though they suspect it might be happening. For example, imagine that a U.S. entity is engaging in a covered data transaction involving data brokerage with a foreign person that is not a covered person and has contractually required 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. The U.S. entity suspects that the foreign person may not be complying with its contractual obligations, but instead of investigating, the U.S. entity deliberately ignores signs or evidence to maintain plausible deniability. Under the rule's ''knowingly'' standard, this U.S. entity can, and should, still be responsible because it purposefully avoided the truth. In other words, the U.S. entity should have known about the violation of the contractual requirements, and taken steps to report it.

Several commenters asked whether § 202.302 would apply to contractual agreements signed before the rule's effective date. If so, they asked for sufficient time for companies to amend those agreements. As discussed in detail in part IV.A.1 of this preamble, the rule will apply to covered data transactions covered by the rule's prohibitions and restrictions that occur after the effective date of the rule, regardless of when U.S. persons signed those agreements. The Department is considering whether to issue a wind-down license that would allow the amendment of any existing agreements that were signed before the rule's effective date but that still allow for a country of concern or covered person to access bulk U.S. sensitive personal data or government related data after the rule becomes effective.

In the final rule, the Department changed the text of this provision to account for the change to the definition of ''covered data transaction'' as described in part IV.B.1 of this preamble. That change limits the term ''covered data transaction'' to transactions involving access by a country of concern or covered person. Because transactions restricted by this section are definitionally not with a covered person, the Department made conforming edits to this provision as well. As with the edits to § 202.301, the revision to § 202.302 clarifies that the provision applies only when the access is by a foreign person, and not in cases where a U.S. person is accessing data from a foreign person. Other than that clarification, these conforming edits do not change the scope of this provision from the proposed rule.

16. Section 202.303—Prohibited Human 'Omic Data and Human Biospecimen Transactions

The NPRM proposed prohibiting 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 to human biospecimens from which such human genomic 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 applied to any of the categories of covered data transactions that involve access to bulk human genomic data or to 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 § 202.303 are never treated as restricted transactions under the rule. As explained in part IV.B.9 of this preamble, the Department has determined to treat transactions involving three additional categories of human 'omic data similarly to human genomic data and has made conforming edits to this section—specifically, changing the reference to ''human genomic data'' to ''human 'omic data.''

The proposed rule solicited comment on whether the Department should exclude transactions involving human biospecimens intended for direct medical use from the rule's prohibition on covered data transactions involving human genomic data and human biospecimens from which such human genomic data could be derived.[104] Multiple commenters expressed their view that the rule should exclude from its definition of ''human biospecimens'' certain human biospecimens intended for direct medical use. Commenters explained that blood-, cell-, and plasma-derived therapeutic products; human organs for transplant; and blood and plasma for transfusions, in particular, provided lifesaving interventions for patients globally, and they highlighted the humanitarian interest of the United States in enabling the transfer of such products to care for patients in countries of concern. Commenters also explained the difficulty of deriving individual human genomic data from human biospecimens used in or processed by finished medical products. The Department agrees with the commenters. As such, the Department revised the definition of ''human biospecimens'' in § 202.223 to clarify that the term does not include human biospecimens intended by the recipient of the human biospecimens solely for use in diagnosing, treating, or

[104] 89 FR 86140.

preventing any disease or medical condition. The prohibition in § 202.303 on covered data transactions with countries of concern or covered persons involving access to bulk human genomic data or human biospecimens from which bulk human genomic data could be derived thus does not prohibit covered data transactions with countries of concern or covered persons involving human biospecimens intended for use by the recipient to diagnose, treat, or prevent any disease or medical condition. In light of this change, a separate exemption for direct medical use is not necessary.

One commenter suggested that the rule permit sharing bulk amounts of human genomic data or human biospecimens from which such data could be derived with countries of concern or covered persons for genetic research where an individual's health or well-being is not at risk—*i.e.,* beyond the diagnosis, treatment, or prevention of a disease or medical condition. The Department declines to adopt an express exemption for data transactions involving human genomic data or human biospecimens from which such data could be derived for general research purposes. Significantly, the rule does not generally prohibit transactions involving access to such data when the recipient is not a covered person or country of concern. For example, citizens of a country of concern who primarily reside in a third country are generally not considered covered persons under the rule. Nor, contrary to some commenters' understanding, does the rule restrict access to publicly available datasets; such data is excluded from the definition of ''sensitive personal data.'' *See* § 202.249(b)(2). The rule also includes important exemptions and is calibrated to permit U.S. persons to share bulk U.S. sensitive personal data, including human genomic data and human biospecimens from which such data could be derived, with countries of concern and covered persons to enable genetics-related research under some circumstances.

For example, data transactions involving human genomic data or human biospecimens from which such data could be derived conducted pursuant to a Federal contract, grant, or agreement, or conducted by a Federal agency, are exempt from subparts C and D of the rule. *See* § 202.504. The rule also exempts from subparts C and D any data transactions to the extent that they are required or authorized by Federal law or pursuant to an international agreement to which the United States is a party, including specified agreements authorizing parties to share global health and pandemic preparedness-related data. *See* § 202.507. The definition of ''covered data transactions'' subject to the prohibitions and restrictions of subparts C and D of the rule identifies specific categories of data transactions to which the restrictions and prohibitions apply, each of which requires a commercial nexus. *See, e.g.,* § 202.214 (''data brokerage'' defined as ''the sale of data, licensing of access to data, or similar commercial transactions involving the transfer of data''); § 202.217 (''employment agreement'' defined as ''any agreement or arrangement in which an individual . . . performs work or job functions directly for a person in exchange for payment or other consideration''); § 202.228 (''investment agreement'' defined as ''an agreement or arrangement in which any person, in exchange for payment or other consideration, obtains direct or indirect ownership interests or rights in relation to'' property or entities); and § 202.258 (''vendor agreement'' defined as ''any agreement or arrangement . . . in which any person provides goods or services to another person . . . in exchange for payment or other consideration''). In addition, §§ 202.510 and 202.511 exempt certain data transactions with countries of concern and covered persons that are necessary to obtain or maintain regulatory approval or authorization to market a drug, biological product, device, or combination product; clinical investigations regulated by the FDA or clinical investigations to support applications to the FDA for marketing or research permits for certain products; and data transactions ordinarily incident to and part of collecting or processing clinical care data or post-marketing surveillance data to support or maintain authorization by the FDA.

In light of the risk identified in the Order, the NPRM, and this preamble of countries of concern seeking to acquire, among other things, U.S. persons' genomic data,[105] the Department declines to adopt a more express exemption for human genomics-related research. However, U.S. persons may seek to obtain a general or specific license pursuant to subpart H if they assess that the prohibitions or restrictions of subparts C and D would apply to specific covered data transactions related to human genomics research involving bulk human genomic data or human biospecimens from which such data could be derived with countries of concern or covered persons.

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

The NPRM proposed prohibiting transactions that have the purpose of evading or avoiding the rule's prohibitions, or that cause a violation of or attempt to violate the rule's prohibitions. The NPRM also proposed prohibiting conspiracies formed to violate the rule's prohibitions. In response to ANPRM comments, the NPRM added new examples 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 AI models. The example in § 202.304(b)(5) involves a U.S. subsidiary of a company headquartered in a country of concern that licenses a derivative algorithm from a U.S. online gaming company for the purpose of allowing the country of concern parent entity to access bulk U.S. sensitive personal data from the training data contained in the algorithm. A commenter raised concerns as to whether the transaction described in the example has the purpose of evading the regulations if the U.S. person subsidiary was licensing an AI classifier that determines whether to advertise to an individual but that does not appear to disclose the sensitive personal data on which it was trained. The commenter recommended that the Department clarify that the prohibited behavior in the example was not licensing a model that was merely trained on bulk U.S. sensitive personal data for the purposes of conducting targeted advertising, but rather licensing a model that reveals the underlying bulk U.S. sensitive personal data upon which it was trained.

As a general matter, the Department agrees that the core question is whether the AI classifier could reveal the underlying bulk U.S. sensitive personal data on which it was trained. For example, if the AI classifier enabled the U.S. person to access the bulk U.S. sensitive personal data on which the model was trained, such as bulk covered personal identifiers, then a licensing transaction intended to evade the rule's prohibitions by enabling the country of concern parent company to access such data could violate the rule. The Department has made revised the example in § 202.304(b)(5) to clarify that point. The Department also agrees that licensing access to an AI classifier that

[105] 89 FR 86118.

could not reveal bulk U.S. sensitive personal data on which it was trained does not violate the rule. Nor does mere access to an algorithm that was trained on bulk U.S. sensitive personal data, by itself, constitute access to the underlying data.

One commenter noted that the example in § 202.304(b)(5) inaccurately states that the licensed algorithm contains training data. The Department agrees and has struck the language ''contained in the algorithm'' from the example.

18. Section 202.215—Directing

The proposed rule defined ''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.

One commenter renewed their observation from the ANPRM that § 202.215 is too broad because it could capture situations where a U.S. service provider does not know or expect their services to be used as part of a covered data transaction. The Department declines to make any further changes to this section because the definition in § 202.215 and the related discussion in the NPRM sufficiently address the commenter's observations, and the commenter does not engage with the NPRM's explanation.[106]

19. Section 202.230—Knowingly

The proposed rule defined ''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 or restricted transactions, the Department stated that it would 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 the proposed rule. As a result of this knowledge standard, the regulations incorporating the word ''knowingly'' do not adopt a strict liability standard.

The Department's decision to adopt a knowingly standard—as opposed to adopting a strict liability standard, which is much more common for IEEPA-based regimes (*e.g.,* OFAC-administered economic sanctions)—reflects the Department's reasoned and balanced approach to mitigating the national security risks described in the Order while taking into consideration the views and concerns of the regulated community. This single, significant decision by the Department sufficiently addresses the source of many of the concerns and observations raised in the comments of this section. With respect to the regulations incorporating this standard, U.S. persons are not responsible for conduct, circumstances, or results that they could not reasonably have known about.

The Department received comments that involved themes or issues that were previously raised and addressed. The Department directs those commenters to relevant discussions in the NPRM. Some comments lacked sufficient factual specificity and were premised on imprecise hypotheticals or generalizations such that it would be unreasonable for the Department to rely on them to make changes to the regulations. Most of these commenters advocated for such sweeping exceptions or amendments to the knowingly standard that, if adopted, would swallow most of the prohibitions and restrictions set forth in the regulations. Such an outcome would not only be at odds with the national security imperatives of the Order but would challenge even a common understanding of what the word ''knowledge'' means. As such, the Department declines to change or amend the standard. The Department continues addressing the relevant comments it received in the continuing discussion.

Nearly all commenters on this provision expressed concern with the ''reasonably should have known'' portion of the standard. The comments seemingly encourage the Department to consent to potentially unreasonable behavior by the regulated community that would be at odds with the national security risks identified in the Order. Commenters argued that ''reasonably should have known'' is susceptible to subjective judgment and hindsight and that the appropriate response to this supposed concern would be to further elevate the standard to ''actual knowledge,'' thereby insulating from liability willfully blind, grossly reckless, or unreasonable actors. These commenters suggested that a U.S. person should not be liable for violating the regulations absent proof of actual knowledge, even if the Department has strong evidence demonstrating that the U.S. person reasonably should have known about, prevented, mitigated, or addressed the violative conduct. Some commenters requested ''safe harbors'' as an alternative to striking or removing the ''reasonably should have known'' language, effectively accomplishing the same outcome if adopted.

The Department declines to make the requested changes. The existing standard provides the necessary flexibility to address national security risks while differentiating responsibilities based on the activities, roles, and characteristics of particular entities and individuals in data transactions. The knowingly standard is already a sufficiently elevated standard (compared to the strict liability standard in other IEEPA-based programs) designed to account for the nature, scope, breadth, volume, and ubiquity of data transactions and the variations in the parties or industries that engage in them. The existing standard also ensures that the Department can discourage, prevent, investigate, and punish conduct that is willfully blind, reckless, or unreasonable in light of the facts and circumstances that give rise to the matter.

The Department also declines to create a safe harbor for due diligence practices at this time. It is possible that as best practices develop over time after the program's effective date, some kind of safe harbor could be included in the regulations. However, at this time, a safe harbor would be premature because there are a wide range of practices in use across multiple industries that may have valuable applications to meeting the requirements of these rules. The Department also notes that after the effective date of the regulations, the Department will be able to entertain and consider detailed license applications and requests for advisory opinions on these and other issues from the commenters and the broader public.

One commenter noted that mitigating risks around the reproduction or disclosure of sensitive data for training AI models is an area of active study and that any current regulation would impede the ability of U.S. companies to deploy AI models. This commenter also suggested that the regulations include an actual knowledge standard for transactions involving AI, that U.S. persons not be required to actively conduct due diligence on data transactions with foreign persons to determine whether they are covered persons,: that an actual, rather than constructive, knowledge standard be

[106] 89 FR 86132.

used in the regulations because of compliance costs, and that clarification be provided as to how liability would apply between a cloud-computing service provider and its customers (the data owners).

This comment lacked sufficient specificity for the Department to address the observation related to the ability of U.S. companies to deploy AI models in the context of this regulation. The commenter also failed to demonstrate how their observations or suggestions regarding not actively conducting due diligence or adopting an actual knowledge standard would mitigate the risk to national security that the Order was intended to mitigate. Additionally, with respect to the commenter's latter concern, the Department directs the commenter to definition of the term ''knowingly'' in § 202.230 along with its various examples. Specifically, Example 5 in § 202.230(b)(5) addresses the situation contemplated by this comment. Thus, the Department declines to make any further changes in response to this comment.

Another commenter observed that the knowingly standard ignores or fails to appreciate the billions of transactions occurring across every country and network of the globe. The comment then described, in the context of cloud computing, the perceived difficulties with determining bulk data thresholds, data content, covered persons, and the three categories of restricted transactions in light of the knowingly standard.

This comment seems to entirely misconstrue how the knowledge standard works vis-à-vis cloud providers and their customers. The Department has not suggested that a cloud provider necessarily be held responsible for whether its U.S. person customers are making their data available via the provider's cloud platform to a country of concern or covered person as part of a restricted transaction. Rather, the Department is seeking to ensure that if a cloud provider itself enters into a restricted transaction by relying on employees or vendors that are covered persons or by taking certain investments from covered persons that would afford those covered persons with access to their customer's bulk U.S. sensitive personal data, then they do so consistent with the requirements of these regulations. As such, the Department makes no changes as a result of this comment.

Another commenter argued that the rule makes problematic assumptions about emerging technologies that the broad ''knowingly'' standard exacerbates. As an example, they pointed to Example 1 in § 202.301(b)(1), arguing that the example assumes that the AI chatbot will reproduce bulk sensitive data. The commenter argued that this assumption leads to the potential that any technology that is vulnerable to attack or misuse would be a covered transaction, and that the overly broad definitions are not conducive to innovation and broad adoption of new technologies. The commenter therefore recommended that the regulations clarify that only data owners, not data resellers such as cloud service providers, are responsible for compliance with the rule, or, in the alternative, that the knowingly standard be limited to actual knowledge.

The commenter's arguments and perspective lack sufficient factual specificity needed for the Department to respond. However, generally, the commenter's concerns are addressed in the NPRM and in parts IV.B.2 and IV.B.19 of this preamble. Additionally, the national security risks that the rule is seeking to address are present regardless of whether the data owner or the data transmitter, such as a cloud-services provider, is the one who provides countries of concern or covered persons access to government-related data or bulk U.S. sensitive personal data. Both such entities can help identify and manage these risks. Given the nature of the risk, the Department declines to further limit the liability of data resellers beyond the current knowingly standard.

C. Subpart D—Restricted Transactions

1. Section 202.401—Authorization To Conduct Restricted Transactions

The NPRM set 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'' defined in § 202.248. The goal of the 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. CISA, in coordination with the Department, developed the requirements—the CISA Security Requirements for Restricted Transactions—which are on the CISA website, as announced via a separate **Federal Register** notice. That document is incorporated by reference into the definition of ''security requirements'' in § 202.248. The 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. The Department of Justice is incorporating by reference the published final security requirements in this final rule. Interested parties can view or obtain CISA's security requirements on CISA's website *https://www.cisa.gov/resources-tools/resources/E.O.-14117-security-requirements.*

One commenter recommended that the Department withhold incorporating by reference CISA's security requirements until after CISA implements an ex parte process to secure input from critical infrastructure sectors. The Department declines to adopt this recommendation. The organizational-, system-, and data-level requirements specified by CISA's security requirements are derived from the existing and commonly used security standards and frameworks that are applied across several critical infrastructure sectors. The CISA security requirements represent an essential component of addressing the risk posed by country of concern and covered person access to government-related data and bulk U.S. sensitive personal data. The application of these security requirements allows the Department to strike the appropriate balance between safeguarding U.S. national security and authorizing employment, vendor, and investment agreements with countries of concern or covered persons. Without the robust safeguards the CISA security requirements provide, the Department would not authorize U.S. persons to engage in restricted transactions, and those transactions would instead be prohibited due to the risk they pose, as discussed below in this part of the preamble. The public has already had several opportunities to comment on and engage with the Department and CISA in meetings before, during, and after the NPRM's comment period to provide input on the security requirements, as discussed in part III of this preamble.

As discussed throughout this preamble, one commenter repeatedly assumed that the restricted transactions are ''low risk,'' criticized the Department's approach to these transactions, claimed that the NPRM's recordkeeping, reporting, and auditing requirements to, for example, retain access logs as a means of compliance,

was tantamount to a ''sweeping surveillance mandate'' for ''billions'' of these ''low risk'' transactions, and argued that the Department should refrain from regulating restricted transactions at this time.

The final rule makes no change in response to this comment. The categories of restricted transactions are not low risk. There is ample open-source and other support for the Department's determination that employee, vendor, and investment agreements involving U.S. persons and countries of concern or covered persons present an unacceptable risk to national security because they may enable countries of concern or covered persons to access government-related data or bulk U.S. sensitive personal data. As discussed in detail in the ANPRM and NPRM, open-source information and examples confirm the Department's determination that each of these three commercial activities, to the extent that they are not otherwise exempt under the rule, are vectors that present unacceptable risk. The comment's assertions that the restricted transactions are ''low risk'' or that there are ''millions'' or ''billions'' of them is not accompanied by any support or analysis, and the comment does not engage with the ANPRM's and NPRM's analysis of this issue. In addition, the comment's assertion about the national security risks posed by particular kinds of transactions necessarily reflects limits on the information available to the public.

The Intelligence Community and other parts of the United States Government have repeatedly warned that foreign adversaries are ''increasing targeting all kinds of data—from personally identifying information, such as your Social Security number, to health and genomic data,'' and that they view such data ''as a strategic resource and collection priority, not only for their own economic advancement, but also for their intelligence and military operations.'' [107] These adversaries ''use every tool in the toolkit—they may recruit an insider, use a cyber intrusion, make an investment, recruit top talent, or do some combination of all of those things,'' and thus they use not only illegal but also ''quasi-legal and even legal tactics[ ]whereby they acquire data through seemingly legitimate investments, partnerships, joint ventures, or regulatory actions.'' [108] In particular, China ''recruit[s] human sources to target our businesses, using insiders to steal the same kinds of innovation and data that their hackers are targeting while also engaging in corporate deception—hiding Beijing's hand in transactions, joint ventures, and investments—to do the same.'' [109] As summarized in more detail in part IV.B.5 of this preamble, the Federal Bureau of Investigation (''FBI'') has explained that companies operating under legal and political systems like the PRC's present a hybrid commercial threat precisely because they can be compelled, influenced, or leveraged to provide access to technology, systems, and data through their commercial activities.

With respect to employees and other individuals with authorized access to sensitive personal data, the United States Government has publicly recognized that foreign intelligence entities ''actively target, solicit, and coerce individuals to obtain information,'' among other things, and that insiders may use their authorized access to harm U.S. national security.[110] For instance, Chinese law authorizes ''national intelligence work agencies'' to use ''any necessary methods, means, and channels'' to carry out ''intelligence work both domestically and abroad,'' including by establishing ''cooperative relationships with relevant individuals and organizations'' and ''entrust[ing] them with related tasks.'' [111] PRC intelligence services often use ''cooperative contacts'' in countries outside of the PRC to further their intelligence goals, including obtaining information concerning foreign companies, politicians, intelligence officers, and political dissidents.[112] In August 2024, for example, a U.S. person pled guilty after obtaining a wide variety of information at the request of Chinese intelligence, including location and other sensitive data about Chinese dissidents, pro-democracy advocates, and members of the Falun Gong religious movement, as well as information about his employer, a major U.S. telecommunications company.[113] Similarly, the United States Government has issued an advisory about the threats posed by IT workers from North Korea, who can ''surreptitiously obtain IT development contracts,'' misrepresent themselves as U.S.-based teleworkers, and ''[u]se privileged access gained as contractors for illicit purposes, including enabling malicious cyber intrusions by other [North Korean] actors.'' [114] With respect to investments, the United States Government has publicly warned that the tactics of countries of concern include using ''mergers, acquisitions, investments, and joint ventures'' to obtain sensitive personal data.[115] This ''include[s] leveraging venture capital (VC) investments, investments through entities based in third countries, investments as limited partners, and iterative minority investments.'' [116] For example, the National Counterintelligence and Security Center (''NCSC'') has publicly assessed that the PRC ''has for years been able to gain access to U.S. healthcare data, including genomic data,'' through channels that include ''investing in U.S. firms that handle sensitive healthcare and other types of personal data, providing them

[107] Michael C. Casey, Dir., Nat'l Counterintel. & Sec. Ctr., *Remarks for the Economic Development Association of Alabama,* 3 (Jan. 30, 2024), *https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL-FINAL-Prepared-Remarks_01302024_Casy_Alabama.pdf* [*https://perma.cc/GZ9F-Z7KE*].

[108] *Id.* at 4, 6; *see also* Nat'l Counterintel. & Sec. Ctr., *Protect Your Organization from the Foreign Intelligence Threat* 1 (Dec. 2021), *https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/12.13.2021%20Protect%20Your%20Org%20from%20the%20Foreign%20Intel%20Threat.pdf* [*https://perma.cc/X9YU-VVHH*].

[109] *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 Counterintel. & Sec. Ctr., *Protecting Critical Supply Chains: Building a Resilient Ecosystem* 2 (Sept. 2024), *https://www.dni.gov/files/NCSC/documents/supplychain/Building-a-Resilient-Ecosystem.pdf* [*https://perma.cc/L7SN-UX8C*].

[110] Nat'l Counterintel. & Sec. Ctr., *supra* note 6, at 7.

[111] *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. 51 ¶ 22, *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.'') (quoting a translation of the National Intelligence Law of the People's Republic of China, promulgated by the Standing Committee of the National People's Congress, June 27, 2017, effective June 28, 2017, amended Apr. 27, 2018).

[112] Press Release, U.S. Dep't of Just., *Florida Telecommunications and Information Technology Worker Sentenced for Conspiring to Act as Agent of Chinese Government* (Nov. 25, 2024), *https://www.justice.gov/opa/pr/florida-telecommunications-and-information-technology-worker-sentenced-conspiring-act-agent* [*https://perma.cc/3L7E-RQRP*].

[113] *See, e.g.,* Plea Agreement, *United States* v. *Ping Li,* No. 8:24–cr–334–SDM–NHA (M.D. Fla. Aug. 19, 2024).

[114] Off. of Foreign Asset Control, U.S. Dep't of Treas., *Fact Sheet: 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*].

[115] Casey, *supra* note 107, at 3; *see also* Nat'l Counterintel. & Sec. Ctr., *Protect Your Organization from the Foreign Intelligence Threat,* 1 (Dec. 2021), *https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/12.13.2021%20Protect%20Your%20Org%20from%20the%20Foreign%20Intel%20Threat.pdf* [*https://perma.cc/X9YU-VVHH*].

[116] Casey, *supra* note 107, at 7.

entry to the U.S. market and access to this data.'' [117] For example, ''China's BGI purchased U.S. genomic sequencing firm Complete Genomics in 2013,'' and in 2015, ''China's WuXi Pharma Tech acquired U.S. firm NextCODE Health to later form WuXi NextCODE Genomics.'' [118] Then, in 2020, the ''U.S. 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.'' [119]

With respect to vendors, the United States Government has publicly assessed that ''contractors, sub-contractors, and vendors that have been granted access to facilities, systems, and networks may wittingly—or unwittingly—do harm to'' an organizations' supply chain.[120] By providing software and other services to U.S. companies, vendors can gain access to sensitive U.S. persons' data for nefarious purposes.[121] DHS has similarly warned that the ''PRC legal and regulatory framework around data offers little to no protection to U.S. firms that share data with PRC firms or entities,'' particularly ''data service providers and data infrastructure'' such as ''data centers owned or operated by PRC firms,'' ''joint ventures'' with PRC firms, and ''software and mobile applications owned or operated by PRC firms.'' [122]

For example:

- In July 2022, news outlets reported that ''Google was sharing potentially sensitive user data with a sanctioned Russian ad tech company owned by Russia's largest state bank'' for four months after the company was sanctioned.[123] According to the reporting, the data Google shared included data about ''users browsing websites based in Ukraine,'' which ''means Google may have turned over such critical information as unique mobile phone IDs, IP addresses, location information[,] and details about users' interests and online activity, data that U.S. senators and experts say could be used by Russian military and intelligence services to track people or zero in on locations of interest.'' [124]
- In July 2021, a Reuters special investigation reported that a Chinese genomics company (BGI Group) ''selling prenatal tests around the world developed them in collaboration with the country's military and is using them to collect genetic data from millions of women.'' [125] According to the report, United States Government advisors warned that the company is amassing ''a vast bank of genomic data'' and ''analy[z]ing [it] with artificial intelligence,'' which could ''potentially lead to genetically enhanced soldiers, or engineered pathogens to target the U.S. population or food supply.'' [126]
- According to a 2021 NCSC assessment, ''Chinese companies have also gained access to U.S. healthcare data by partnering with hospitals, universities, and other research organizations in America. These U.S. entities routinely seek low-cost genomic sequencing services for their facilities, which Chinese biotech firms can often provide due to Chinese government subsidies . . . These partnerships allow U.S. entities to expand their research capabilities, while Chinese firms gain access to more genetic data on more diverse sets of people, which they can use for new medical products and services.'' [127] For example, ''[o]ver the past decade, China's BGI has partnered with many research and healthcare entities in America to provide them with genomic sequencing services, while also gaining access to health records and genetic data on people in the U[nited] S[tates].'' [128] And ''[i]n July 2020, the U.S. 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.'' [129]

More broadly, employee, vendor, and investment relationships have been vectors exploitable and exploited by countries of concern to access critical infrastructure, technology, trade secrets and intellectual property, research, and other assets. For example, on August 8, 2024, a Federal grand jury returned an indictment against a U.S. person for facilitating a scheme to deceive American and British companies into hiring foreign remote IT workers who were actually North Korean actors. The companies paid the North Korean actors hundreds of thousands of dollars that were funneled to North Korea for its weapons program.[130] And in March 2024, a Federal grand jury indicted a Chinese national for theft of trade secrets. As a Google software engineer, the individual was granted access to Google's confidential information related to the hardware infrastructure, the software platform, and the AI models and applications they supported. Between 2022 and 2023, he uploaded and transferred over 500 sensitive files, including proprietary hardware and software data used by Google's AI supercomputing systems for machine learning. The individual sent this data to his personal account while secretly traveling to China, working for two PRC-based companies in the AI industry, and eventually founding his own AI company in China while still serving as a Google employee. The individual had another Google employee swipe his work-issued access badge to make it appear that he was working from his U.S. Google office when, in fact, he was in the PRC.[131]

Other examples include the following:

- In September 2018, journalists reported that China's antitrust authorities raided a U.S. chemical company's Shanghai office, demanding access to the company's research network, passwords, and printed document; seizing computers; and intimidating employees. The raids came one year into an arbitration battle between the U.S. company and its former Chinese joint venture partner, who the U.S. company suspected had obtained and was using the U.S. company's proprietary technology without permission. The Chinese antitrust investigators pressured the

[117] Nat'l Counterintel. & Sec. Ctr., *supra* note 67, at 2.

[118] *Id.*

[119] *Id.* at 3.

[120] Nat'l Counterintel. & Sec. Ctr., *supra* note 109, at 5.

[121] *See, e.g.,* U.S. Dep't of Commerce, Final Determination: Case No. ICTS–20121–002, Kaspersky Lab, Inc., 89 FR 52434, 52436 (June 24, 2024) (describing how Kaspersky employees gained access to sensitive U.S. person data through their provision of anti-virus and cybersecurity software).

[122] U.S. Dep't of Homeland Sec. *supra* note 57, at 2, 10–12.

[123] Craig Silverman, *Google Allowed a Sanctioned Russian Ad Company to Harvest User Data for Months,* ProPublica, (July 1, 2022), *https://www.propublica.org/article/google-russia-rutarget-sberbank-sanctions-ukraine* [*https://perma.cc/6R4V-L868*].

[124] *Id.*

[125] Kirsty Needham & Clare Baldwin, *Special Report: China's Gene Giant Harvests Data From Millions of Women,* Reuters (July 7, 2021), *https://www.reuters.com/article/world/special-report-chinas-gene-giant-harvests-data-from-millions-of-women-idUSKCN2ED1A5/* [*https://perma.cc/3VPW-AP5D*].

[126] *Id.*

[127] Nat'l Counterintel. & Sec. Ctr., *supra* note 67, at 2.

[128] *Id.* at 3.

[129] *Id.*

[130] Press Release, U.S. Dep't of Just., *Justice Department Disrupts North Korean Remote IT Worker Fraud Schemes Through Charges and Arrest of Nashville Facilitator* (Aug. 8, 2024), *https://www.justice.gov/opa/pr/justice-department-disrupts-north-korean-remote-it-worker-fraud-schemes-through-charges-and* [*https://perma.cc/Z4P2-G7TN*].

[131] Press Release, U.S. Dep't of Just., *Chinese National Residing in California Arrested for Theft of Artificial Intelligence-Related Trade Secrets from Google* (Mar. 6, 2024), *https://www.justice.gov/opa/pr/chinese-national-residing-california-arrested-theft-artificial-intelligence-related-trade* [*https://perma.cc/R88W-RBAU*].

U.S. company to drop the arbitration case to resolve the antitrust investigation, seemingly as part of a broader strategy to exert control over foreign companies and their intellectual property.[132]

• In 2018, the *New York Times* published an article detailing how a U.S. semiconductor company, Micron, was the target of intellectual property theft in Taiwan. After Micron rejected acquisition and partnership offers by Chinese chipmakers in 2015, Fujian Jinhua Integrated Circuit Company (a Chinese company) and UMC (a Taiwanese company) partnered to build a chip making factory in China. Jinhua tapped UMC to develop the necessary technology and UMC allegedly recruited Micron employees, who stole propriety information from Micron before leaving the company. Micron filed a lawsuit against UMC and Jinhua in the United States, accusing them of trade secret theft. UMC denied the allegations, but Taiwanese police raided UMC offices and recovered the stolen documents and devices. Meanwhile, Jinhua and UMC filed a patent infringement lawsuit against Micron in China, which could block Micron's sales in the country.[133] The Micron case is emblematic of how the Chinese government uses every legal and regulatory lever—poaching talent, subsidies, patent infringement, antitrust, outright theft, and the courts—to pressure individual companies to transfer technology or not pursue cases of theft.

• In March 2019, Tesla accused a former engineer of stealing intellectual property from the company's self-driving car project and providing that information to a Chinese electric vehicle startup company. The individual allegedly copied more than 300,000 files and directories, repeatedly logged into Tesla's networks, and cleared his browser history before leaving Tesla for the rival employer.[134]

With adversaries' increasing strategic focus on Americans' sensitive data as one of the assets to fuel their intelligence and military activities, it should come as no surprise that they would use the same vectors to access companies, systems, and other repositories of sensitive personal data. In light of the risks to government-related data and bulk U.S. sensitive personal data posed by employment, vendor, and investment agreements, the Department considered outright prohibiting transactions conducted through those vehicles. The Department believes that, given the gravity of the threats and the plethora of examples where countries of concern have exploited these vehicles to obtain access to U.S. person data, the risks would justify such prohibitions. However, because the Department has determined that the security requirements can adequately mitigate these risks, the rule characterizes these transactions as restricted transactions.

The same commenter claimed that while the NPRM had well defined objectives for what they characterized as ''high-risk'' prohibited transactions, objectives were not well-defined for what they characterized as ''low-risk'' restricted transactions. This commenter concluded that this could result in: (1) forcing companies to decrypt encrypted data, thereby undermining U.S. data security and cybersecurity; (2) requiring the aggregation of vast quantities of sensitive personal and non-personal data, creating further cybersecurity risks; (3) criminalizing and deterring ordinary business transactions with U.S. allies; and (4) impeding low-risk information sharing with U.S. allies needed for scientific, health, or other purposes. The Department has already addressed the mischaracterization of risk by this commenter, so this point will not be readdressed.

In response to the commenter's other points, first, the Department reiterates that nothing in the rule imposes a legal requirement to decrypt or aggregate data to comply. The NPRM extensively explained this point, and the commenter did not engage with that explanation at all or offer any substantive analysis to support the commenter's claim. The Department expects companies to ''know their data'' but has been clear throughout this rulemaking process that decryption is not a required step in that effort. Indeed, other commenters that will be subject to this rule have acknowledged that there is no need to decrypt encrypted data. For example, during at least one of the Department's engagements with stakeholders, a public-interest research center acknowledged that the proposed rule would not require companies to decrypt their data to know whether they are regulated or to comply.

Second, the Department expects companies to know their data when they are dealing in government-related data and bulk U.S. sensitive personal data. 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, data-using entities typically 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.[135] 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.[136]

Third, the rule does not criminalize or deter ordinary business transactions with U.S. allies. As discussed in part IV.F.1 of this preamble, the fact that the rule has cross-border ramifications for companies located in countries that are not countries of concern due to the ownership networks of covered persons and countries of concern and covered persons speaks to the pervasive reach of covered persons and countries of concern. Their ability to influence and compel access, or obtain it through these ownership structures, which span across countries and continents provides further support for the need to address this risk to our national security.

Another commentor recommended that the Department clarify that the provisions regulating restricted transactions are intended to address the risks attendant in allowing covered persons access to covered data, but are

[132] Lingling Wei & Bob Davis, *How Chinese Systematically Pries Technology from U.S. Companies,* Wall Street Journal (Sept. 26, 2018), *https://www.wsj.com/articles/how-china-systematically-pries-technology-from-u-s-companies-1537972066.*

[133] Paul Mozur, *Inside a Heist of American Chip Designs, as China Bids for Tech Power,* New York Times (June 22, 2018), *https://www.nytimes.com/2018/06/22/technology/china-micron-chips-theft.html* [*https://perma.cc/B3L4-NNNM*].

[134] Sherisse Pham *Tesla Is Accusing a Former Employe of Stealing Self-Driving and Giving It to a Chinese Rival* CNN (Mar. 22, 2019), *https://www.cnn.com/2019/03/22/tech/tesla-xiaopeng-motors-lawsuit/index.html* [*https://perma.cc/W76V-QT88*].

[135] 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,* Privacy 108 (Nov. 14, 2023), *https://privacy108.com.au/insights/data-tagging-for-security/* [*https://perma.cc/8PQA-89DA*]; Nat'l Inst. 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*].

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

not intended to prevent access by the covered person. Although this comment does not require any change to the rule, the restricted transactions are classes of transactions that would be prohibited except to the extent they comply with CISA's security requirements, which are designed to mitigate the risk of access to government-related data or bulk U.S. sensitive personal data. As CISA's final security requirements explain, the security requirements are meant to prevent access to covered data by countries of concern or covered persons unless specific efforts outlined in the security requirements are taken to minimize the national security risks associated with such access. As further explained by CISA, the security requirements accomplish this goal by requiring U.S. persons to implement a combination of mitigations that, taken together, are sufficient to fully and effectively prevent access by covered persons or countries of concern to sensitive personal data that is linkable, identifiable, unencrypted, or decryptable using commonly available technology, consistent with the required data risk assessment. That could be accomplished, as the security requirements explain, by denying access outright or by only allowing covered persons access to sensitive personal data for which regulated persons have instituted other data-level requirements that mitigate the risks of countries of concern or covered persons obtaining direct access to the underlying government-related data or bulk U.S. sensitive personal data (in addition to applying the organizational and system-level requirements).

The Department expects that complying with the security requirements will not ordinarily result in a de facto prohibition on restricted transactions and instead would typically permit restricted transactions to go forward. As CISA's final security requirements point out, a U.S. business could choose to fully deny a covered person access to government-related data or bulk U.S. sensitive personal data while still executing a restricted transaction that would otherwise allow access to the business's networks and systems. For example, a U.S. business that holds bulk U.S. sensitive personal data could accept an investment from a covered person or hire a covered person as a board director (a restricted transaction) by complying with the security requirements to deny or otherwise mitigate the covered person's access to that data. The covered person in those restricted transactions could perform their responsibilities without access to that data (or with access to that data if the regulated entities have instituted adequate data-level requirements, in addition to the organizational and system-level requirements).

To be sure, it is possible that, in what the Department expects to be relatively rare circumstances, the only service that a covered person would be providing as part of a restricted transaction would require access to data that is linkable, identifiable, unencrypted, or decryptable using commonly available technology, such that complying with the security requirements would preclude that transaction. Because compliance with the security requirements would preclude the provision of the service, the restricted transaction in that circumstance may be effectively prohibited, absent the grant of a specific license authorizing it. That result would be consistent with the unacceptable national security risks of allowing covered persons to access the underlying data.

Some commenters provided feedback on the security requirements that would govern restricted transactions. The Order makes CISA, not the Department, responsible for developing the security requirements. The Department has shared with CISA any comments that are relevant to the security requirements but were erroneously filed in the docket for this rulemaking.

2. Section 202.258—Vendor Agreement

The proposed rule defined 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.

A commenter sought clarification on whether the rule would apply to U.S.-based third-party cloud-computing service platforms that provide storage and IT services. The term ''vendor agreement'' refers to a kind of activity, not a kind of entity. The provision of cloud-computing services falls squarely within the definition of ''vendor agreement.'' As explained in part IV.B.19 of this preamble, a U.S. person providing cloud-computing services, would, like any other U.S. person, be prohibited from engaging in its own covered data transactions that are prohibited or restricted by the rule.

The same commenter also suggested adding an exemption for cloud service providers or clarifying whether the knowledge standard would be met if a customer manages their data independently. The Department declines to add such an exemption, noting that the rule aims to protect access regardless of the services offered, and any exemption would not sufficiently mitigate the associated threats. The application of the ''knowing'' standard to cloud services is discussed separately in part IV.B.19 of this preamble.

The same commenter sought clarity on whether the restrictions on vendor agreements extend to subsidiaries or affiliates of U.S. companies located in countries of concern. As explained in part IV.F.1 of this preamble, a U.S. company's foreign subsidiary, organized under the laws of or with its principal place of business in a country of concern, is a separate entity from its U.S. parent. As Example 6 in § 202.256(b)(6) shows, the U.S. parent would be a U.S. person, and the subsidiary would be a covered person. As a result, the U.S. parent would generally be restricted from engaging in a vendor agreement with its covered person subsidiary if that agreement provides the subsidiary with access to government-related data or bulk U.S. sensitive personal data. No change to the rule is required in response to this request for clarification.

3. Section 202.217—Employment Agreement

The proposed rule defined 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.

One commenter suggested that the Department delete § 202.217 and instead exempt employment agreements from the scope of the rule. The commenter noted that employment agreements are contracts signed between enterprises and individuals and made the unsupported assertion that a restriction on employment agreements with citizens of countries of concern or non-American citizens living in countries of concern is a discriminatory policy that infringes on individuals' equal employment rights and violates their human rights. The Department declines to implement this change.

The inclusion of employment agreements within the scope of restricted transactions is related to the national security risk articulated in the NPRM. As noted, the legal and political regimes of countries of concern enable

them to compel employees who work for their companies or within their territory to share information with these governments, including their intelligence services, creating a significant risk to U.S. national security. Further, the rule itself does not prohibit employment agreements with individuals in a country of concern or employed by a covered person, but rather simply requires that the CISA security measures be in place to ensure that those covered person employees cannot access government-related data or bulk U.S. sensitive personal data that is linkable, identifiable, unencrypted, or decryptable using commonly available technology by covered persons and/or countries of concern, consistent with the required data risk assessment.

This rule is not discriminatory. It does not turn on racial, ethnic, or national identity; instead, the rule identifies categories of covered persons based on the risk that a country of concern could leverage such a person or entity to access government-related data or bulk U.S. sensitive personal data. The criteria in § 202.211(a) does not indiscriminately apply, for example, to everyone of Chinese nationality. To the contrary, covered person categories distinguish between non-U.S. citizens who primarily reside in a country of concern (who are covered persons because they are subject to the jurisdiction and legal regimes of the country of concern's government); non-U.S. citizens who are not primarily resident in a country of concern (who are only covered persons if they work for a country of concern or covered person, or are individually designated); and anyone located in the United States (who are not covered persons, unless designated, because of the weaker categorical ability of countries of concern to subject them to the country of concern's jurisdiction or to otherwise direct or control their actions). As such, the rule adopts the proposed approach from the NPRM without change.

One commenter asked for ''additional clarification regarding exemptions related to a Chinese national that receives employment, particularly for instances where Chinese nationals are employed in the United States and go through the immigration process.'' Although this question is not entirely clear, the commenter appears to be asking whether the provisions regarding restricted transactions would apply to an employment agreement between a country of concern's national and a U.S. company while the national's application for a change of immigration status is pending. The answer depends on several additional facts. If the Chinese national is employed in the United States and is living in the United States, then the individual meet the definition of a U.S. person, which includes ''any person in the United States.'' As such, the individual is not a foreign person and would therefore not meet the criteria of any of the categories of covered persons (unless individually designated). In this scenario, therefore, the employment agreement between the Chinese national and the U.S. company would not be a restricted transaction because it is between two U.S. persons.

By contrast, if the Chinese national is primarily resident in a country of concern, works outside the United States for the government of a country of concern or for another covered person, or has been designated as a covered person, then the individual would be a covered person. In that scenario, as a result, the employment agreement between the Chinese national and the U.S. company would be a restricted transaction. The fact that the Chinese national has applied for a pending change of U.S. immigration status would not alter that individual's status as a covered person. With respect to a change in immigration status, the national would become a U.S. person under § 202.256 (and thus lose their status as a covered person, unless designated) only upon an actual change in—not mere application for a change in—their status such that they are ''admitted to the United States as a refugee under 8 U.S.C. 1157 or granted asylum under 8 U.S.C. 1158'' or become a U.S. citizen, national, or lawful permanent resident. No change to the rule is necessary to clarify this point.

The same commenter remarked that the provisions on restricted transactions ''impose substantial constraints on employment agreements in countries of concern, potentially creating compliance challenges that extend beyond U.S. jurisdiction.'' The commenter noted that these restrictions could hinder the legal structuring of employment agreements, which must also adhere to foreign regulatory requirements, and urged the Department to consider adjustments to the regulations to avoid conflicts with foreign data protection laws. First, the Department clarifies that the rule regulates U.S. persons engaging in covered data transactions that involve employee agreements with covered persons or countries of concern and does not target employment agreements ''in countries of concern.'' Next, the commenter did not provide support or analysis for their assertions that the rule imposes substantial constraints that would potentially hinder entering into such agreements or create conflicts with foreign data protection laws. The Department reiterates that the rule does not prevent employment agreements with covered persons or countries of concern, but instead requires U.S. companies to meet certain security requirements and other applicable requirements. Lastly, the Department finds unpersuasive the commenter's argument that making companies adhere to foreign regulatory requirements would hinder the legal structuring of employment agreements, as navigating domestic and foreign regulations and provisions is inherent in the nature of engaging in cross-border business, even separate from this rule.

Another commenter asked the Department whether unpaid service on a volunteer board would be considered ''other consideration.'' The value and benefit derived from one's experience can constitute ''other consideration'' as part of an exchange for services rendered, even if on a volunteer basis or for charitable or humanitarian purposes. No change has been made to this provision as a result of this comment.

One commenter noted that while the NPRM discussed the regulations on the employment of covered persons by U.S. companies, clarification is needed regarding the employment of covered individuals by non-U.S. affiliated companies. Generally, the provisions of § 202.401 regulate U.S. persons engaging in restricted transactions involving an employment agreement with a country of concern or covered person. Absent evasion or avoidance scenarios, or fact patterns wherein a foreign person causes a U.S. person to violate the provisions of this rule, foreign persons are not restricted from engaging in employment agreements with covered persons. No change to the rule is necessary in response to this comment.

This same commenter also asked for clarification on the extent to which the rule would apply to a foreign entity that includes U.S. affiliates. The commenter did not provide enough specificity or facts for the Department to meaningfully address this question (such as the relationship between the foreign entity and the U.S. affiliates, whether the foreign entity is a covered person, and the nature of the transactions at issue). In general, however, any affiliate is a separate entity that, like a subsidiary, would have to be independently analyzed to determine whether it meets the definitions of U.S. person, foreign person, or covered person. To the extent that the commenter has a more specific question, the commenter can seek an advisory opinion.

Another commenter recommended that the Department clarify that the term ''employment agreement'' does not extend to roles that do not have or that are unlikely to have access to covered data by virtue of covered data transactions, such as office, human resources, or other functions that the commenter says are an essential part of regular business processes and that would not otherwise be covered by the exemption for corporate group transactions. Under § 202.401, a restricted transaction prohibits U.S. persons from knowingly engaging in a covered data transaction involving an employment agreement with a country of concern or covered person, unless the U.S. person complies with the security requirements and all other applicable requirements. Where there is no covered data transaction, the employment agreement is not a restricted transaction, even if the employee is a covered person. This same commenter also sought confirmation of whether it would be a restricted transaction involving an employment agreement for a U.S. person company to provide access to basic company information, such as a company staff directory, to business offices in a country of concern. The commenter did not provide enough information to assess the potential outcome. As such, the Department advises this commenter to seek an advisory opinion, following the provisions of § 202.901.

Finally, another commenter asked whether the outcome in Example 4 in § 202.217 would change if the data scientist hired by the financial services company were developing a new AI-based personal assistant as part of the provision of financial services, not as a standalone product that could be sold to the company's customers. The Department presumes that this commenter's question was whether the financial services exemption in § 202.505 would apply and the answer is no. A covered person data scientist, who is provided administrator rights allowing that covered person to access, download, and transmit bulk quantities of personal financial data, is not an exempt transaction because it is not ordinarily incident to the provision of financial services. Similarly, sharing such data with a covered person for the purpose of developing a new AI-based personal assistant is not ordinarily incident to the provision of financial services. Furthermore, as noted in the NPRM, the Department does not believe that an employment agreement or a vendor agreement that gives a covered person access to bulk U.S. 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. The Department makes no change to the rule in response to this comment.

4. Section 202.228—Investment Agreement

The proposed rule defined 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 excluded 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 excluded from ''investment agreement'' investments (1) in any publicly traded security, in any security offered by any investment company that is registered with the U.S. Securities and Exchange Commission (''SEC''), such as index funds, mutual funds, or 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, in the NPRM, the Department shared that it was considering a range of different proposals, including de minimis percentages that are significantly lower or higher than this percentage, such as the five 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). The Department invited public comment on the specific de minimis threshold that should be used in this exception for passive investments.

Two commenters advocated for a higher de minimis threshold. These comments urged the Department to adopt a 25-percent threshold, contending that it aligns with the Financial Crimes Enforcement Network's rules for reporting beneficial owners, as well as with the proposed rule's annual reporting requirement for U.S. entities engaging in restricted transactions involving cloud-computing services where the U.S. entities are 25 percent or more owned by a country of concern or covered person.[137] The commenter also asserted, without support, that this threshold is unlikely to give an investor a degree of control that threatens national security. The other commenter urged the Department to adopt a 35-percent threshold, noting that numerous minority investments have more than 10 percent of total voting and equity interest but are still entirely passive.

The Department has considered the commenters' input but does not believe that increasing the threshold to 25 or 35 percent would sufficiently address the national security risks that the rule seeks to address. Twenty-five or 35-percent ownership could potentially provide an investor meaningful economic leverage or informal influence over access to a company's assets (like sensitive personal data) even when the investor does not obtain formal rights, control, or access beyond standard minority shareholder protections. For example, an investor may have sufficient voting power to influence a company's decision-making, whether formally through shareholder voting, or informally based on the size of the investment, the investor's interest in the company's success, and the company's interest in maintaining or expanding the investment. This informal influence is exactly the type of leverage that the investment agreement category of restricted transactions seeks to address.

Furthermore, the Financial Crimes Enforcement Network rules for reporting beneficial ownership are primarily designed to address risks posed by shell and shelf entities to the U.S. financial system to prevent, for example, money laundering and illicit finance, which are different than the kind of risk this rule seeks to address.[138] Similarly, the rule's annual reporting requirement for certain restricted transactions is not comparable. The annual reporting

[137] *See* 3 CFR 1010.380; 89 FR 86153.

[138] Beneficial Ownership Information Reporting Requirements, 87 FR 59498, 59498 (Sept. 30, 2022) (to be codified at 31 CFR pt. 1010) (stating that the rule's requirements are intended to prevent and combat money laundering, terrorist financing, corruption, tax fraud, and other illicit activity).

requirement provides the Department with information about companies with notable country of concern ownership that access large amounts of sensitive personal data; it does not speak to the applicability of the rule to a broad category of transactions, as the investment agreement definition does. In contrast, CFIUS regulations, which also focus on the national security risks accompanying foreign investments into U.S. companies, do not, in certain circumstances, extend to passive investments where the investments are less than 10 percent of outstanding voting interests and do not include certain rights, such as involvement in substantive decision-making.[139] One commenter noted that the passive investment exclusion extends to publicly-traded companies and pooled investment funds and does not cover one-percent, passive, minority investments into private U.S. entities. The commenter suggested carving out these investments on the basis that they are truly passive, noting that the exclusion's third prong, which requires that the investment does not give a covered person rights beyond those reasonably considered to be standard minority shareholder protections, ensures that the investments are passive. The Department agrees and has modified the requirements of the investment agreement exclusion for passive investments in § 202.228(b)(iii) to include limited partner investments into private entities. For these reasons, the Department slightly expands the scope of the passive investment exclusion and adopts a de minimis threshold of 10 percent in the final rule.

D. Subpart E—Exempt Transactions

The NPRM proposed exempting several classes of data transactions from the scope of the proposed rule's prohibitions. The final rule adopts those exemptions with some modifications as discussed in part IV.D of this preamble. The final rule also makes clear that the due-diligence, auditing, reporting, and recordkeeping requirements in subpart J and the auditing requirements in subpart K generally do not apply to exempt transactions. One exemption, in § 202.510 for regulatory approval data, is available only to the extent that the U.S. person complies with specified recordkeeping and reporting requirements. The generally applicable requirement in § 202.1104 for U.S. persons to report rejected transactions applies to all prohibited transactions; an otherwise exempt transaction would not be prohibited. The Department also retains its generally applicable authority in § 202.1102 to request and subpoena information. The other requirements in subparts J and K are intended to apply only as conditions of engaging in restricted transactions and has clarified this through additional language in each exemption listed in subpart E.

1. Section 202.502—Information or Informational Materials

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.'' [140] 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.[141] Section 2(b) of the Order delegated this statutory authority to the Attorney General, and the Department exercises this authority to define ''information or informational materials.'' The Department received few comments on its proposed interpretation. For the reasons explained below and in the NPRM, the final rule adopts the definition proposed in the NPRM without change, including with respect to information not fully created and in existence at the time of the transaction. The Department has, however, changed the definition of ''sensitive personal data'' in response to comments received on this topic to exclude certain metadata.

One commenter asserted that the Department's interpretation would not be entitled to deference after the Supreme Court's decision in *Loper Bright Enterprises* v. *Raimondo*.[142] The Court's decision in *Loper Bright* explicitly preserved the Executive's authority to reasonably define statutory terms when Congress has delegated to the Executive the authority to do so.[143] The Court explained that it was the judiciary's responsibility to determine whether Congress had done so. Here, Congress was explicit in its delegation of authority to the Executive Branch to issue ''regulations prescribing definitions'' as ''may be necessary for the exercise'' of IEEPA authorities.[144] This express delegation is similar to those examples identified by the Court as delegating authority to define terms.[145] In any event, for the reasons explained by the Department in the NPRM and reiterated here, the Department believes its interpretation is the best interpretation of the statutory term in light of text, structure, and context, including the enactment history and legislative history.

As set out in the NPRM, the Department defines ''information or informational materials'' as 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 and with IEEPA's broader purpose to limit material support to adversaries. *See* § 202.226. A broader definition of the term would enable adversaries and countries of concern to use non-expressive data to undermine our national security.

Some commenters believed that this interpretation is inconsistent with the Berman Amendment. As set out in detail in the NPRM, the Department disagrees. Briefly, the Berman Amendment's list of examples of information and informational materials reflects Congress' intent to protect the import or export of expressive speech and communicative works and mediums that may be carrying such expressive content.[146] This is reinforced

[139] 31 CFR 800.302(b) (providing that ''covered control transactions'' do not include ''a transaction that results in a foreign person holding 10 percent or less of the outstanding voting interest in a U.S. business . . . but only if the transaction is solely for the purpose of passive investment.''); 31 CFR 800.243 (defining ''solely for the purpose of passive investment'' as indicating ownership interests that do not, *inter alia,* afford any rights that if exercised could constitute control or any access, rights, and involvement specified in 31 CFR 800.211(b)); 31 CFR 800.211(b) (specifying access, rights or involvement to include board membership observer rights, or involvement in substantive decision-making).

[140] 50 U.S.C. 1704.

[141] *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).

[142] 144 S. Ct. 2244 (2024).

[143] *Id.* at 2263 (''[S]ome statutes ''expressly delegate[ ]'' to an agency the authority to give meaning to a particular statutory term.'').

[144] 50 U.S.C. 1704.

[145] *Loper Bright,* 144 S. Ct. at 2263 n.5 (quoting 29 U.S.C. 213(a)(15) (''as such terms are defined and delimited by regulations of the Secretary'') and 42 U.S.C. 5846(a)(2) (regulating according to term ''as defined by regulations which the Commission shall promulgate'').

[146] One commenter insisted that the ''ordinary meaning'' of the term, including as reflected in an Office of Management and Budget (''OMB'') circular, includes non-expressive data. The cited OMB circular post-dates the enactment of the Berman Amendment and defines the term for use in guidance to agencies for managing Federal IT resources. It is therefore of exceedingly negligible relevance here. As explained at length in the NPRM, the term ''information and informational materials'' as used in the Berman Amendment cannot be understood outside the specific history and context surrounding its enactment. Some commenters pointed out that some mediums

Continued

by the Berman Amendment's legislative and drafting history and context, which reveal Congress's focus on expressive materials (such as artwork, literature, or news media) and on the free exchange of ideas. In particular, in enacting the 1994 changes to the Berman Amendment, Congress explicitly acknowledged and ratified a meaning of the term ''information or informational materials'' that was narrower than anything that, in a colloquial or dictionary sense, could potentially be characterized as ''information or informational materials.'' [147]

One commenter contended that information—including the non-expressive data subject to this rule—would be protected by the First Amendment as speech and is therefore categorically within the Berman Amendment's prohibition. But whether the non-expressive data subject to this rule would be subject to First Amendment analysis does not dictate whether it falls within the scope of the Berman Amendment. As the legislative history and context make clear, Congress intended with the Berman Amendment to advance core First Amendment principles, not to wholesale import First Amendment doctrine as such. This commenter's suggestion is flatly inconsistent, for example, with Congress's conscious preservation of the exception that allows the Executive Branch to regulate information—even expressive information—that is not fully created at the time of the transaction. That legislative choice demonstrates a degree of flexibility reflected in, though not necessarily coterminous with, First Amendment doctrine.

Nor does the Department's interpretation contradict the First Amendment orientation of the Berman Amendment or impermissibly burden the First Amendment rights of U.S. persons. The rule is analogous to the wide range of content-neutral and viewpoint-neutral laws regulating commercial transactions involving the sale, disclosure, and use of sensitive personal data that courts have consistently upheld against First Amendment challenge. As the Supreme Court observed long ago, ''numerous examples'' of commercial information ''are regulated without offending the First Amendment.'' [148] Courts have consistently held that the First Amendment permits viewpoint-neutral restrictions on commercial transactions that use, disclose, and sell confidential financial information; targeted marketing lists of consumers, customers' purchase, rental, and borrowing histories for books, videos, and other materials; telecommunication customers' proprietary network information; personal dossiers aggregated from public and nonpublic information; and consumer-reporting information.[149] Similarly, these types of transactions are not protected from export restrictions under IEEPA by the Berman Amendment.

In sum, the Department's definition appropriately ''balances IEEPA's competing purposes'' in ''restricting material support for hostile regimes while encouraging the robust interchange of information.'' [150] The export of non-expressive data (including the sensitive personal data that the rule regulates) 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.

In the NPRM, the Department explained that, under its interpretation, expressive content and associated metadata that is not sensitive personal data would be categorically outside the scope of the definition of ''sensitive personal data'' and thus outside the scope of the regulations, regardless of the type of activity (or transaction) involved. The Department asked for further comments on this issue, and several commenters suggested that further protections for metadata ordinarily included in expressive materials, such as geolocation data embedded in digital photographs, were warranted. The Department agrees that it is appropriate to provide further protections for the export of metadata that is ordinarily associated with expressive materials, or that is reasonably necessary to enable the transmission or dissemination of expressive materials, to avoid unintended effects on the export of information or informational materials. Such metadata is therefore categorically excluded from the rule's scope, as reflected in revisions to the definition of ''sensitive personal data'' in § 202.249. The rule would still properly reach metadata that is not ordinarily associated with expressive materials or not reasonably necessary to its transmission or dissemination because regulating that data does not impermissibly prohibit the export of the expressive material itself. This prevents the abuse of expressive materials as a conduit for transmitting unrelated government-related data or bulk U.S. sensitive personal data. The Department reiterates that other aspects of the rule (such as bulk thresholds or the definition of ''covered data transaction'') also protect the dissemination of expressive content and its associated metadata.

listed—such as CD ROMs or microfiche—can store non-expressive data just as well as expressive content. This is undoubtedly true but misses the point: Congress listed these media types because they are used to store the expressive content such as music, artwork, or literature that the provision seeks to protect. One commenter contended that the Department's proposed definition does not account for the distinct terms ''information'' and ''informational materials.'' The Department disagrees: the phrase refers to expressive content (''information'') as well as the mediums containing that content (''informational materials'').

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

[148] *Ohralik* v. *Ohio State Bar Ass'n,* 436 U.S. 447, 456 (1978).

[149] *E.g., Dun & Bradstreet, Inc.* v. *Greenmoss Builders, Inc.,* 472 U.S. 749 (1985); *id.* at 762 (three-justice plurality opinion agreeing that ''[t]here is simply no credible argument that this type of credit reporting requires special protection to ensure that debate on public issues will be uninhibited, robust, and wide open'') (cleaned up); *id.* at 764 (Burger, C.J., concurring in the judgment) (agreeing); *id.* at 774 (White, J., concurring in the judgment) (agreeing that ''the defamatory publication in this case does not deal with a matter of public importance'' warranting First Amendment protection). *See also Trans Union LLC* v. *FTC,* 295 F.3d 42, 46, 52–53 (D.C. Cir. 2002) (upholding the constitutionality of the FTC's regulations implementing the privacy protections of the Gramm–Leach–Bliley Act by restricting financial institutions' use of any personally identifying information obtained by financial institutions in connection with providing financial products or services to a consumer); *Trans Union Corp.* v. *FTC (Trans Union I),* 245 F.3d 809, 818 (D.C. Cir. 2001), reh'g denied; *Trans Union Corp.* v. *FTC (Trans Union II),* 267 F.3d 1138, 1142 (D.C. Cir. 2001), cert. denied, 536 U.S. 915 (2002); *Boelter* v. *Hearst Commc'ns, Inc. (Hearst II),* 269 F. Supp. 3d 172, 177–78 (S.D.N.Y. 2017); *Boelter* v. *Hearst Commc'ns, Inc. (Hearst I),* 192 F. Supp. 3d 427, 445 (S.D.N.Y. 2016); *Boelter* v. *Advance Magazine Publishers, Inc.,* 210 F. Supp. 3d 579, 599 (S.D.N.Y. 2016); *Nat'l Cable & Telecommc'ns Ass'n* v. *FCC,* 555 F.3d 996, 1001 (D.C. Cir. 2009) (restrictions on disclosure of customer proprietary network information); *Brooks* v. *Thomson Reuters Co.,* No. 21–cv–01418–EMC, 2021 WL 3621837, at *1, *15 (N.D. Cal. Aug. 16, 2021); *King* v. *Gen. Info. Servs., Inc.,* 903 F. Supp. 2d 303, 309–11 (E.D. Pa. 2012).

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

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 administrative processes for seeking an advisory opinion or applying for a specific license before engaging in the transaction.

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

The NPRM proposed exempting 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 exempts grantees and contractors of Federal departments and agencies, including the Department of Health and Human Services (''HHS''), 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.

Two commenters noted that the rule would hinder scientific progress by preventing international collaboration with scientists who are primarily resident in countries of concern because those scientists would no longer be able to leverage large population neuroscience datasets funded by the National Institutes of Health (''NIH''). One of these commenters noted that the proposed rule could impose unwanted administrative burdens on U.S. researchers by creating roadblocks to data sharing and thereby potentially decrease the global competitiveness of U.S. genetics research and related applications. These concerns are unsupported. As explained in parts IV.D.2, IV.D.4, and IV.D.8–10 of this preamble, the rule regulates certain categories of commercial transactions and does not prohibit or restrict United States research in a country of concern, or research partnerships or collaboration with covered persons, that does not involve the exchange of payment or other consideration as part of a covered data transaction. In addition, the rule includes exemptions and provisions meant to streamline compliance and reduce the impact on researchers. The rule exempts expressive information and personal communications, such as the posting or publication of health-related research data online by individual researchers. To the extent that such covered data transactions are conducted pursuant to a grant, contract, or other agreement entered into with the United States Government, that activity would be exempt from the prohibitions and restrictions of the rule. And the rule exempts the activities of the United States Government, such as providing access to its own databases. The rule exempts data that is lawfully publicly available or available in unrestricted, open-access repositories and other widely distributed media, such as databases freely available to the scientific community. Other exemptions include clinical care data and post-marketing surveillance data needed for FDA authorization, submissions of regulatory approval data to research or market drugs, biological products, devices, and combination products, and the sharing of data as part of international agreements (including those addressing pandemic preparedness and global health surveillance). The Department therefore does not believe that the rule will undermine the global competitiveness of the U.S. genetics sector significantly, if at all.

To the contrary, the rule is intended to limit the ability of countries of concern and covered persons to use commercial means to obtain and exploit access to government-related or bulk U.S. sensitive personal data. Safeguarding government-related data and bulk U.S. sensitive personal data is crucial for maintaining trust and competitiveness within the research community. These regulations will foster international collaboration and strengthen the global standing of U.S. researchers. Furthermore, the rule does not prevent the sharing of data with countries that are not countries of concern. It only requires that U.S. persons require foreign persons that are not countries of concern or covered persons, and with which the U.S. persons engage in covered data transactions involving data brokerage to contractually require that the foreign person refrain from subsequent data transactions involving data brokerage of the same data with a country of concern or covered person, as described in § 202.302(a)(1). Foreign persons that obtain covered data from U.S. persons should be contractually prohibited from onward transfer of this data to countries of concern or covered persons.

The rule's prohibitions and restrictions, as limited by this and other exemptions, are considerably less onerous and wholly different in kind than those imposed by certain other countries. For example, a PRC set of laws and regulations supposedly aimed at protecting national security, data security, and privacy impose strict controls on transfers of certain broad categories of data collected or produced in China—including vaguely defined categories like ''important data''—to places outside of China, effectively localizing such data. To the extent that these authorities do not prohibit cross-border transfers of such data outright, they generally subject such transfers to review, approval, and security assessments conducted by PRC government regulators and require that the recipient be contractually obligated to follow security measures prescribed by the government.[151] Transfers of scientific data outside of China are also subject to government review and approval. In addition, the European Union's (''EU'') General Data Protection Regulation (''GDPR''), which the EU calls ''the toughest privacy and security law in the world,'' [152] imposes restrictions on the transfer of personal data outside the European Economic Area that are designed to ensure that the level of protection of individuals

[151] These laws include 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), *see* Exh. A to Newman Decl., *supra* note 111; 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), *see* Exh. B to Newman Decl., *supra* note 111; 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), *see* Exh. C to Newman Decl., *supra* note 111; the National Intelligence Law of the People's Republic of China (promulgated by the Standing Committee of the National People's Congress, June 27, 2017, effective June 28, 2017, amended Apr. 27, 2018), *see* Exh. D to Newman Decl., *supra* note 111; and 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), *see* Exh. E to Newman Decl., *supra* note 111.

[152] Ben Wolford, *What Is GDPR, the EU's New Data Protection Law?, GDPR.eu, https://gdpr.eu/what-is-gdpr/* [*https://perma.cc/3L4B-CTPQ*].

granted by the GDPR remains the same, among other restrictions.[153]

Some commenters requested clarity about projects receiving both federal and non-Federal funding, as well as the extent to which the exemption would include transactions conducted pursuant to a grant, contract, or other agreement with Federal departments and agencies to conduct and share the results of federally funded research that also involved grants, donations, or other funding from non-Federal entities, like private institutions or donors. The Department has added new examples in § 202.504 to clarify that transactions conducted pursuant to a grant, contract, or other agreement with Federal departments and agencies are exempt, even if those transactions also involve funding from non-Federal entities.

3. Section 202.505—Financial Services

The NPRM proposed exempting 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.

Commenters were generally supportive of the Department's inclusion of a financial services exemption. Comments requested clarifications about the exemption's scope and outer peripheries, requested changes to its examples or requested new examples, and suggested changes that would expand its applicability beyond data transactions that are ordinarily incident to and part of the provision of financial services. The Department has made many of these changes and clarifications to the exemption and its examples in response to these comments. Some commenters raised issues that failed to appreciate the applicability of the regulations' other exemptions or provisions and made suggestions that would be redundant or unnecessary if accepted. Other commenters mistakenly treated the list of financial services as exhaustive and failed to appreciate that it is an exemplary list. Some commenters failed to appropriately consider how the suggestions or observations they put forth would address the national security risks the Order was intended to mitigate. Other commenters failed to explain why it was essential in the context of their suggestions that covered persons or countries of concern access government-related data or bulk U.S. sensitive personal data.

In the NPRM, the Department also shared that it was 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. As the Department explained, under this proposed 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.[154] The Department shared two new proposed examples and sought public input as to whether to treat those examples as exempt transactions or restricted transactions.[155] Specifically, the Department sought public comment on 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 bulk U.S. 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. One of the new examples proposed in § 202.505(b)(12) of the NPRM featured a U.S. wealth-management services company that collects bulk personal financial data on U.S. clients, appoints a citizen of a country of concern located in a country of concern to its board, and allows this board member access to the bulk personal financial data in connection with the board's data security and cybersecurity responsibilities.

One commenter stated that, for banking organizations, it would treat that example as ''ordinarily incident to and part of'' the provision of financial services because board oversight of a bank's programs is integral to its required governance procedures. However, the commenter also emphasized that a director carries out an oversight function with respect to a firm's security program as a core component of risk management, is not involved in day-to-day management activities, and does not have a need to access bulk U.S. sensitive personal data to faithfully carry out his or her roles and responsibilities. In explaining the commenter's rationale that a director would not need access to this data to perform his or her duties, the commenter overlooked one of the key facts in the example—that the board director could access bulk personal financial data of the company's U.S. person clients. Treating this board director's employment as a restricted transaction would only mean implementing the security requirements, including data-level requirements that mitigate the risk that the director may access data that is linkable, identifiable, unencrypted or decryptable using commonly available technologies, and which the commenter confirms the director does not need access to. It does not prohibit the board director's employment. Accordingly, the Department has decided to treat the transactions in the proposed examples as restricted transactions because, as stated in the NPRM, 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 bulk U.S. 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. *See* §§ 202.505(b)(3)

[153] *See* 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. 44; see also *International data transfers,* European Data Protection, *https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en* [*https://perma.cc/G5A3-4HEB*] (''In a nutshell, the GDPR imposes restrictions on the transfer of personal data outside the EEA, to non-EEA countries or international organisations, to ensure that the level of protection of individuals granted by the GDPR remains the same.'').

[154] *Cf., e.g.,* 31 CFR 560.405(c) (discussing the OFAC exemption for transactions ''ordinarily incident to a licensed transaction'' as applied to scenarios involving the provision of transportation services to or from Iran); 31 CFR 515.533 n.1 (discussing the 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, Dir., 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).

[155] 89 FR 86135.

and 202.505(b)(12). 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.

Commenters suggested that financial institutions engage in operational and compliance activities that are uncommon to other sectors. Because of this, the commenters believe there may be confusion on the applicability of the exemptions for financial services and corporate groups transaction. To address this supposed confusion, the commenters recommended the expansion of the financial services exemption to include data transactions that are ordinarily incident to and part of the operations of financial services entities regulated by Federal or State banking or insurance regulators, without limitation. The Department declines to adopt this suggestion. First, the suggestion is too broad and appears to fully exempt financial-services entities (*i.e.,* their operations) from the regulations, even if they engage in the same covered data transactions that pose the unacceptable risks addressed by the Order (such as selling bulk U.S. sensitive personal data to a covered person). As the NPRM explained, the rule takes an activity-based approach, not an entity-based approach, because it is these commercial activities (*i.e.,* transactions) that pose an unacceptable national security risk, regardless of the kind of entity that engages in them. A new Example 6 was added in § 202.506(b)(6) to address the issue of the overlap between these exemptions. There is no tension or confusion between these independent exemptions because any combination of the exemptions can apply, depending on the circumstances of any given matter. In addition, to the extent that a financial-services entity (or any other U.S. person) engages in data transactions that are required or authorized by Federal law (*e.g.,* the Bank Secrecy Act), those transactions could also be exempt under § 202.507.

Similarly, commenters requested that the financial services exemption be expanded to expressly include data transfers arising from a financial institution's regulatory obligations. This change appears unnecessary. The exemption in § 202.507 already authorizes ''data transactions to the extent they are required or authorized by Federal law.'' Example 1 in § 202.507(d)(1) addresses the commenters' concerns by making clear that a U.S. bank or other financial institution can engage ''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).'' Some commenters also mentioned that the Department may be inadvertently limiting the relevant scope of exempted data transactions in § 202.505 to those arising from securities-based financial services subject to Securities Exchange Commission (''SEC'') jurisdiction. The list of financial services in the exemption is exemplary, not exhaustive, given that the defined term ''including'' precedes the list. However, to avoid the possibility of any substantial misunderstanding as to whether activities related to commodity markets can be financial services, the Department has added ''securities and commodity markets'' to the parenthetical in § 202.505(a). The Department also confirms that financial services include futures, options, and derivatives subject to the jurisdiction of the Commodity Futures Trading Commission (''CFTC''), security-based swaps, and the activities of Futures Commission Merchants, commodity trading advisors, introducing brokers, and other CFTC-regulated entities. Parties that face continued challenges determining whether their activities are financial services will be able to file requests for advisory opinions with the Department after the effective date of the regulations.

These same commenters were also concerned that the exemption may not reach transactions involving mortgage-backed securities and other asset-backed securities, which could curtail the ability of parties in countries of concern from buying securities backed by U.S. mortgages and other assets. This comment appears to be based on a misunderstanding. As the Example 2 at § 202.505(b)(2) makes clear, it is ordinarily incident to and part of securitizing and selling asset-backed obligations (such as mortgage and nonmortgage loans) to a covered person for a U.S. bank to provide bulk U.S. sensitive personal data to the covered person. As such, this activity would be exempt, and no changes seem necessary.

Some commenters suggested that cybersecurity services may be considered ancillary to processing payments and funds transfers, based on the view that such services are a form of risk mitigation and prevention. Commenters also proposed the addition of a new example to clarify the limitations in Example 4 at § 202.505(b)(4) regarding product development in what appears to be fraud detection and prevention models. The Department agrees that cybersecurity services performed in conjunction with the processing of payments and funds transfers can be ordinarily incident to the provision of financial services and thus exempt to the extent that they are performed as part of the processing of payments and funds transfers. The Department, however, declines to extend the exemption to product development or adopt an additional example specific to product development. The comment does not explain why bulk U.S. sensitive personal data needs to be accessed in a country of concern or by a covered person to develop such products as part of providing financial services in a country of concern or to a covered person. The Department makes no further changes regarding this issue.

Several commenters requested clarifications to Example 10 in § 202.505(b)(10). The commenters suggested a clarification that the financial services exemption covers lawful regulatory requests from countries of concern directed at any financial services provider, not just banks. The financial services exemption is not limited to any specific entity and applies to any transaction by any entity that is ordinarily incident to and part of providing financial services, and thus no change is necessary. Nevertheless, as clarification, the Department adopts the suggestion to broaden Example 10 from ''bank'' to ''financial services provider'' and adds language showing that sharing financial data as part of routine regulatory reporting requirements is ordinarily incident to the provision of financial services and is therefore exempt.

Commenters also noted that the current version of the financial services exemption is ambiguous as to whether it covers the transfer of personal financial data or covered personal identifiers incidental to the purchase and sale of goods and services, since such exempted transactions must be ''ordinarily incident to and part of the provision of financial services'' and, as such, the text of the rule appears to narrowly focus on financial-services institutions or payment processors rather than sellers in those marketplaces. This comment misapplies the exemption. The exemption applies to any transaction that is ordinarily incident to and part of financial services, which includes any transaction that is ordinarily incident to and part of the transfer of personal financial data or covered personal identifiers for the purchase and sale of goods and services. As Example 5 in § 202.505(b)(5) makes clear, the financial services exemption is not only applicable to the activities of

financial institutions; that example shows that the exemption can apply to a U.S. company operating an online marketplace.

Commenters also suggested renaming § 202.505 as ''financial services and consumer transactions for goods or services'' and making the following modifications: in § 202.505(a), before '', including,'' insert ''or purchase and sale of goods or services.'' The Department declines to implement these changes, which appear unnecessary in light of the rule's text and examples, and which may inadvertently broaden the exemption to cover vendor agreements that the rule intends to regulate.

4. Section 202.506—Corporate Group Transactions

The NPRM proposed exempting covered data transactions to the extent that 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 (such as sharing employees' covered personal identifiers for human-resources purposes; payroll transactions, such as 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).

One commenter requested that the Department clarify its definitions of ''subsidiary,'' ''affiliate,'' and ''branch.'' Although these terms are not defined in the rule, the Department provided clarification on their meaning in section IV.C.4 of the NPRM.[156] The commenter does not identify any meaningful ambiguity or specific uncertainty about the application of these terms, which are commonly used and applied terms throughout other national security programs. As a result, the Department does not believe it is necessary or appropriate at this time to define these terms. To the extent that ambiguities or uncertainty about the application of these terms arises in the future, the Department can issue general guidance, and the public can seek advisory opinions on their application to specific transactions.

Numerous commenters requested that the Department broaden the scope of data transactions covered by this exemption to cover, as one commenter put it, ''more corporate substantive operations-related activity,'' rather than only data transactions that are ordinarily incident to and part of administrative or ancillary business operations. For example, one commenter suggested that the scope of this exemption be broadened ''to encompass a broader range of necessary business activities beyond routine administrative support.'' Similarly, multiple commenters requested that this exemption be expanded to cover data sharing required for global business operations or services. Other commenters similarly requested that this exemption be expanded to cover any data transfers ''necessary to a company's business,'' even if such activity is not ordinarily incident to and part of administrative or ancillary business operations, or to ''all instances where a subsidiary in a country of concern receives data from a U.S.-based parent.'' 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.

In addition, numerous commenters requested that the Department make clear that certain specific data transactions or activities identified by the commenters, including what some commenters referred to as ''routine'' and ''low-risk'' transactions, are included within the scope of this exemption. These included internal collaboration and review platforms; pricing and billing systems; customer and vendor relationship management tools, including technical assistance centers; expense monitoring and reporting; recruiting and other activities related to identifying and selecting job applicants; contingent workforce management; and financial planning, analysis, and management activities.

The list of ancillary business activities in the exemption is not exhaustive and therefore, some of these activities, such as expense monitoring and reporting, are likely already covered by the scope of this exemption. As such, the Department declines to incorporate these suggestions, as doing so is unnecessary. Additionally, while some of the suggested transactions may be routine, it is unclear why these functions would need to be utilized or performed by a covered person or are necessary for a company to operate in a country of concern. The Department anticipates addressing which activities fit within the exemption through public guidance issued after publication of the final rule.

One commenter requested that the Department include in the exemption transfers of government-related data or bulk U.S. sensitive personal data to corporate affiliates in countries of concern for routine research and development purposes and not related to other exemptions, including §§ 202.510 and 202.511. The Department declines to adopt this recommendation. This commenter did not provide enough information for the Department to assess the scope or economic, scientific, or humanitarian value of any such transactions, nor the likelihood that such transactions would otherwise satisfy the definition of a ''covered data transaction'' to fall within the scope of the rule. In light of the substantial risks posed by country of concern access to government-related data and bulk U.S. sensitive personal data described in part II of this preamble and in the NPRM,[157] the Department declines to expand the corporate group transactions exemption to include data transactions involving government-related data and bulk U.S. sensitive personal data with corporate affiliates of U.S. companies in countries of concern for routine research and development purposes.

One commenter reiterated their comment on the ANPRM seeking clarification that the corporate group transactions exemption would cover all employees of a U.S. entity and its affiliates in countries of concern, as well as employees of trusted vendors. The corporate group transactions exemption applies to transactions, not to individuals. As discussed in the NPRM, this exemption may apply to situations in which employees of a U.S. company's affiliate located in a country of concern are provided with access to covered data.[158] Additionally, for the reasons discussed in section IV.C.4 of the NPRM,[159] the Department declines to broaden the corporate group transactions exemption to include suppliers and other third-party vendors. This commenter also reiterated their comment on the ANPRM seeking confirmation that business offices in a particular country of concern that have access to basic company information, such as a company staff directory, would be covered by this exemption. This scenario is discussed in section IV.C.4 of the NPRM.[160]

Multiple commenters requested that the Department include an example in § 202.506 involving a U.S. financial-services provider that has a subsidiary located in a country of concern. In this

[156] 89 FR 86136.

[157] 89 FR 86118–19.

[158] 89 FR 86218.

[159] 89 FR 86136.

[160] *Id.*

example, customers of the U.S. company conduct financial transactions in the country of concern, and customers of the foreign subsidiary conduct financial transactions in the United States. To perform customer service functions related to these financial transactions, the foreign subsidiary accesses bulk U.S. sensitive personal data—specifically, personal financial data.

The Department agrees that the corporate group transactions exemption would apply to the foreign subsidiary's access to the personal financial data under these circumstances because it is ordinarily incident to and part of the provision of customer support. The Department has added this example to § 202.506(b). The Department also notes that the transaction described by these commenters would be covered by the financial services exemption.

One commenter asked the Department to clarify whether the corporate group transactions exemption would apply to a situation in which a U.S. financial-services provider has a foreign affiliate that is also a financial-services provider. In this scenario, the two entities have a centralized risk-monitoring application used by global fraud risk-control employees to effectively monitor fraud risk across the enterprise. The U.S. company allows the foreign affiliate's employees conducting fraud risk monitoring to access bulk U.S. sensitive personal data to the extent reasonably necessary to ensure effective enterprise-wide risk monitoring. The Department agrees that the corporate group transactions exemption would apply to this scenario. While the transaction is between a U.S. company and its affiliate, effective enterprise-wide risk monitoring is ordinarily incident to and is an ancillary part of providing financial services.

This commenter also asked the Department to clarify whether this exemption would apply to a situation in which a U.S. company has a foreign affiliate that is a covered person and that provides customer support services to U.S. customers as part of global customer support operations. In this scenario, the U.S. company provides the foreign affiliate with access to bulk U.S. sensitive personal data to the extent necessary for the affiliate to provide customer support. The commenter considered the foreign affiliate's access to bulk U.S. sensitive personal data to be covered by the corporate group transactions exemption because, the commenter believed, such access was ordinarily incident to and part of the provision of customer support.

The Department does not agree that the foreign subsidiary's access to bulk U.S. sensitive personal data under the circumstances described by this commenter would be covered by the corporate group transactions exemption. Specifically, the Department does not consider the foreign subsidiary's access to the bulk U.S. sensitive personal data to be ordinarily incident to and part of the provision of customer support because, in the scenario described by the commenter, the foreign subsidiary appears to be providing customer support to the U.S. company's customers in all instances—including instances in which customer support is being provided to U.S. persons located in the United States—and not just in instances that involve a country of concern or a covered person. This view aligns with the Department's view on the inapplicability of the financial-services exemption to vendor agreements where the underlying financial services being provided by the vendor do not involve a country of concern or a covered person, as discussed in section IV.C.3 of the NPRM [161] and Example 4 in § 202.505(b).

One commenter requested that the Department clarify that ''potential incidental access to physical facilities'' containing covered data would not be considered ''access'' to such data. This commenter provided an example in which a counterparty employs a repair technician who is not authorized to access facilities that transmit U.S. sensitive personal data ''but theoretically could obtain unauthorized access.''

This comment lacks the specificity needed to justify a change or evaluate a suggestion and does not provide support or analysis. As discussed in the NPRM, the definition of ''access'' is intentionally broad.[162] Section 202.201 of the 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'' (emphasis added). The commentor has not offered any suggestion for a way to distinguish between incidental or inadvertent access in a manner that would minimize the national security risk that this rule seeks to address. Finally, the CISA security requirements contemplate organizational, system, and data-level security requirements that are meant to prevent access by covered persons or countries of concern to data that is linkable, identifiable, unencrypted, or decryptable using commonly available technology. For these reasons, the Department declines this commenter's request.

One commenter urged the Department to remove or lessen the requirement in this exemption that additional access protocols be established to ensure that employees in countries of concern only have access to pseudonymized, anonymized, or de-identified data. This commenter noted that many companies have already instituted robust security and data governance measures, as well as mechanisms for intra-affiliate data transfers, and may have contractual or other legal obligations to comply with when storing or safeguarding data. The application of this exemption does not require that data be pseudonymized, anonymized, or de-identified. As noted in section IV.C.4 of the NPRM, however, a non-exempt employment agreement that qualifies as a restricted transaction would be subject to the CISA security requirements incorporated in § 202.248.[163]

This commenter also remarked that Examples 4 and 12 in §§ 202.505(b)(4) and 202.505(b)(12) (the financial services exemption) should be covered by the corporate group transactions exemption. This commenter provided no support or analysis for this assertion, and the comment lacks the specificity needed to justify a change or evaluate a suggestion. There is no indication in these examples that they involve data transactions 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.

One commenter asked the Department to clarify whether this exemption would apply to data transfers that are necessary for business-data analysis purposes, noting that it would be burdensome for a company to have to implement a different data analysis system since a shared system is both vital to operations and most cost-effective. This comment lacks the specificity needed to justify a change or evaluate a suggestion. In addition, the business-data analysis mentioned by this commenter appears not to be ancillary or administrative activity but rather part of a company's core business activities, such as product development and research. The Department declines to exempt such

[161] 89 FR 86135.

[162] 89 FR 86122.

[163] 89 FR 86136.

activities as explained in the NPRM and part IV.D of this preamble.

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

The NPRM proposed exempting 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 are necessary for compliance with Federal law.

One commenter expressed concern that companies could exploit this exemption by relying on data transfer rules contained in expansive digital trade agreements. This commenter expressed alarm about the possibility that certain provisions of such agreements, which reflect commitments to cross-border data transfers, could be used as a basis to circumvent the prohibitions and restrictions in this rule, especially since the list of international agreements in § 202.507(a) is not exhaustive. Accordingly, this commenter requested that the Department clarify that this exemption does not cover transactions required or authorized by international trade agreements.

The Department appreciates this commenter's recognition of the nexus between the provisions in digital free trade agreements, on the one hand, and the national security risk that the Order and this rule seek to address, on the other hand. The Department agrees and reiterates that the exemption contained in § 202.507(a) for sharing data pursuant to international agreements would not allow for the sharing of government-related data or bulk U.S. sensitive personal data with a country of concern pursuant to the World Trade Organization's General Agreement on Trade in Services or other trade agreements. As explained in the NPRM, digital-trade agreements and arrangements that merely facilitate international commercial data flows—such as the Global Cross-Border Privacy Rules and Global Privacy Recognition for Processors Systems of the Global Cross-Border Privacy Rules Forum and the Asia-Pacific Economic Cooperation (''APEC'') Cross-Border Privacy Rules and APEC Privacy Recognition for Processors Systems—are outside the scope of the exemption for international agreements. As the NPRM explained, these arrangements consist of frameworks for coordinating national regulatory measures, prohibit data localization, and do not facilitate the sharing of data between the United States and a country of concern.[164]

Another commenter suggested that this exemption be expanded to cover data transactions not only to the extent that they are required or authorized by Federal law, but also to the extent that they ''facilitate or otherwise relate to compliance'' with Federal law or other regulatory obligation. This commenter noted that some financial institutions may institute compliance programs that go beyond what is specifically required by Federal law in order to help ensure compliance with such laws or other regulatory obligations.

The Department appreciates that some financial institutions may impose internal rules and requirements that are stricter than those established by Federal law in order to help ensure compliance. The commenter's suggestion to extend this exemption to data transactions to the extent that they ''facilitate or otherwise relate to'' compliance with Federal law or other regulatory obligations, however, lacks the specificity needed to justify a change. It does not, for example, identify any specific non-exempt covered data transactions with countries of concern or covered persons that go beyond what is required or authorized by Federal law but that would be prohibited or restricted. Accordingly, the Department declines to modify this exemption.

Some commenters requested that the Department include a separate mechanism in § 202.507(b) for researchers to share data rapidly during a public health crisis, if such sharing is not otherwise authorized by the specific mechanisms identified in that section. The Department declines to adopt this recommendation. As explained in parts IV.B.2 and IV.D.9 of this preamble, the rule does not prohibit or restrict the sharing of data by researchers or others that does not involve the exchange of payment or other consideration as part of a covered data transaction. In addition, the rule already has exemptions—including for sharing data as authorized or required by the International Health Regulations (which address data sharing for public health events and emergencies), the Pandemic Influenza Preparedness and Response Framework, the Global Influenza Surveillance and Response System, and other health-related international agreements—that allow data sharing in these circumstances. Finally, general and specific licenses are available to the extent that the sharing of government-related data or bulk U.S. sensitive personal data in these circumstances would involve non-exempt prohibited or restricted transactions.

6. Section 202.509—Telecommunications Services

The NPRM proposed regulating exempt transactions that are ordinarily incident to and part of telecommunications services.

Several commenters suggested that the Department expand the definition of ''telecommunications services'' in § 202.252 to include voice and data communications over the internet. The Department agrees. Instead of limiting the scope of ''telecommunications services'' to the definition in 47 U.S.C. 153(53), the Department has adopted its own definition of the term to more appropriately cover present day communications for the purposes of the exemption in § 202.509. This new definition includes the provision of voice and data communications services regardless of format or mode of delivery such as communications services over IP, voice, cable, wireless, fiber, or other types of broadband. This definition is limited to communications services and does not reach services like cloud computing.

One commenter recommended expanding the definition of ''telecommunications services'' to include data transactions that are ordinarily incident to the function of communications networks, effectively creating an exemption for IP addresses. The Department appreciates that IP addresses are ubiquitously used to track users on the internet. However, the Department currently views IP addresses as an important listed identifier that can be used to track users and devices as a personal identifier as well as to provide precise geolocation data. Therefore, the Department declines to expand this exemption to include communications networks.

Another commenter recommended expanding this exemption to include the provision of cybersecurity services, noting that network-based identifiers used in cybersecurity services function similarly and do not involve the personal data of users. While the Department appreciates the importance of cybersecurity services, the Department declines to make this suggested change. First, whether network-based identifiers themselves involve personal data is not the relevant inquiry. Network-based identifiers can be exploited, in combination with other listed identifiers, to harm national security in the ways identified in this preamble. Second, some network-based identifiers, such as ''IMEI'' numbers and

[164] *See* 89 FR 86136–37.

Integrated Circuit Card Identifiers (''ICCID'') are used in other contexts and often do contain other sensitive personal data. Third, the exemption already exempts transactions to the extent that they are ordinarily incident to and part of providing telecommunications services. The comment does not identify the specific non-exempt transactions with countries of concern or covered persons involving the provision of cybersecurity services that would be prohibited or restricted, nor does the comment explain why the sharing of government-related data or bulk U.S. sensitive personal data with countries of concern or covered persons is an integral part of those transactions. Therefore, no changes were therefore made in response to this comment.

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

The NPRM exempted certain data transactions necessary to obtain and maintain regulatory approval from country of concern regulatory entities to market a drug, biological product, medical device, or combination product. The Department sought public comment on the scope of the exemption, including whether to authorize covered data transactions involving covered person vendors in countries of concern that are involved in submitting regulatory approval data on behalf of U.S. persons to country of concern regulators; the extent to which regulatory approval data includes personally identifiable information; and the definition of ''regulatory approval data.''

This exemption in the final rule is limited to data that is de-identified or pseudonymized consistent with FDA regulations; 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 or pseudonymized data that is gathered in the course of a clinical investigation and would typically be required for 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, typically would fall outside the scope of the exemption because such data is not reasonably necessary to evaluate covered product safety or effectiveness. One commenter identified some circumstances where such data might be relevant, such as when the data is collected by a wearable device, or when tracing contaminated or defective products. The Department appreciates this comment and agrees that the data necessary to evaluate safety or effectiveness may vary with circumstances. No change to the regulatory text is necessary, however, as the text already incorporates a ''reasonableness'' standard.

One commenter pointed out that the preamble to the NPRM indicated that the exemption extended to data required to obtain or maintain ''authorization or approval'' to ''research or market'' the specified products, whereas the proposed regulatory text did not include the term ''authorization'' or ''research.'' The Department has revised the text of § 202.510 to include both terms, consistent with its stated intent in the NPRM to exempt submissions to regulatory bodies to conduct certain medical research and consistent with the definition provided for the term ''regulatory approval data.''

This commenter also sought clarification that the exemption applies to inspections by country of concern regulatory bodies and that, in these circumstances, the de-identification requirement should not apply. This commenters explained that regulatory bodies, including both the FDA and those in countries of concern, possess investigatory authority to more closely examine data related to clinical investigations or post-marketing activities, and that when they exercise this inspection authority, they ordinarily are granted access to all data—including data that has not been de-identified or pseudonymized—consistent with current FDA and foreign regulatory bodies' practices. The Department first confirms that regulatory inspections, when necessary to maintain authorization or approval to research or market a covered product, generally would fall within the scope of the exemption. The Department appreciates the comment regarding the release of unredacted, identifiable bulk U.S. sensitive personal data in the context of these inspections; such data would generally fall outside the scope of the exemption, even when accessed as part of a regulatory inspection. The comment does not provide information on the frequency of these inspections by country of concern regulators, the extent of U.S. sensitive personal information that would be exposed, the manner in which inspectors or regulatory agencies obtain or retain that data, or who, as a practical matter, the relevant parties ordinarily would be. For example, the rule does not generally apply to transactions that do not involve a U.S. person; it is unclear from the information provided whether or how the rule would apply where the regulatory body conducts an investigation of an in-country clinic or vendor. Although the comment refers generally to the possibility and authority to conduct overseas inspections, the comment does not suggest that such inspections occur with any frequency. The Department is therefore not convinced that a broad regulatory exemption allowing country of concern regulators unrestricted access to bulk U.S. sensitive personal data adequately accounts for the corresponding national security risks. The Department will continue to evaluate this concern, including the appropriateness of a general license.

Several commenters sought clarification of whether ''key-coded'' or pseudonymized data would qualify as de-identified data under this provision (and under § 202.511) and suggested that the Department align the requirement with the FDA's requirements for data submission. Commenters explained that pseudonymized data is used by researchers to enable, for example, longitudinal studies and data traceability. As these commenters recognize, the data submitted to the FDA typically does not include ''names and other information which would identify patients or research subjects,'' 21 CFR 20.63(b), while other provisions explain (for example) that certain submissions should ''assign a unique code for identification of the patient,'' 21 CFR 314.80(i), instead of using patient names. The Department appreciates these comments. The risks of re-identification when using pseudonymized or key-coded data are generally higher than when using fully de-identified data. But given the importance of being able to associate patient data longitudinally, the FDA's practice in this regard, and the established industry protocols for preserving patient or subject anonymity, the Department has changed this provision—as well as the corresponding limitation to de-identified data in § 202.511—to apply to both de-identified data and pseudonymized data as described in 21 CFR 314.80(i). 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. 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 also 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 or authorization from a country of concern. One commenter requested that this be codified in the regulatory text; the Department sees no need to do so because nothing in the regulatory text requires otherwise.

The exemption is limited to transactions that are necessary to obtain or maintain regulatory approval or authorization to market or research a drug or other medical product. Commenters requested additional clarity about whether the exemption would apply to the use of a registered agent, country of concern third-party vendors, employees of a U.S. company in a country of concern, or U.S. subsidiaries incorporated in a country of concern to submit regulatory approval data to country of concern regulators. The Department agrees that there is a strong humanitarian interest in ensuring that U.S. persons may share regulatory approval data with country of concern regulators or covered persons as necessary to obtain or maintain authorization to market drugs, biological products, devices, or combination products. The exemption in § 202.510 does so. The Department has revised Example 3 in § 202.510 to clarify that sharing regulatory approval data with a registered agent, country of concern subsidiary of a U.S. company, or an employee of a U.S. company who primarily resides in a country of concern that a U.S. company intends for the registered agent, subsidiary, or employee to submit to a country of concern regulator, as required by country of concern law, is exempt because it is ''necessary'' to obtain approval or authorization. In contrast, Example 4 of § 202.510 illustrates that entering into a vendor agreement with a covered person to store and organize regulatory approval data for eventual submission to a country of concern regulator is not ''necessary'' to obtain regulatory approval if it is not required by country of concern law. The Department has added Example 5 to clarify that the exemption would also apply to de-identified sensitive personal data collected during post-marketing product surveillance to assess the safety and efficacy of a drug and submitted to a country of concern regulator by a local country of concern registered agent, pursuant to country of concern law, for a U.S. company to maintain authorization to market the drug in the country of concern.

The Department recognizes that some U.S. persons seeking to market drugs, biological products, devices, or combination products in a country of concern may engage third-party vendors to assist with the submission of such data to regulatory entities. The exemption in § 202.510 is calibrated to enable such arrangements where it is ''necessary'' to obtain or maintain regulatory approval from a country of concern regulator and where such data is de-identified or pseudonymized, consistent with FDA regulations, and reasonably necessary for the country of concern regulator to assess the safety and effectiveness of such products. One commenter suggested changing the exemption to include transactions that are ''reasonably necessary'' to obtain or maintain approval, but the full comment suggests that there would be substantial difficulty in divining the line between transactions that are ''reasonably necessary'' and those that are simply ''convenient.'' Given the substantial national security risks that the prohibitions and restrictions are intended to mitigate, the Department believes that a facially narrower exemption is appropriate. Moreover, in many cases, transactions such as these may likely proceed as restricted transactions under subpart D. Recognizing the complexity of country of concern laws and business practices associated with submitting regulatory approval data to country of concern regulators, the Department declines to provide further specificity about what data transactions it deems ''necessary'' to obtain or maintain regulatory authorization to market drugs, biological products, devices, or combination products. The final rule provides U.S. persons the opportunity to seek advisory opinions about specific, concrete data transactions, including the use of covered person third-party vendors, and general or specific licenses to authorize any such data transactions otherwise subject to subparts C and D. *See* §§ 202.801, 202.802, and 202.901.

Some commenters requested that the Department exempt, under either § 202.510 or § 202.511, data transactions where a U.S. company has licensed the intellectual property of a country of concern pharmaceutical company to market—including potentially conducting a clinical investigation for—a country of concern-developed drug in the United States. The commenters explained that such licensing agreements may require the U.S. company to submit adverse effects reports or other clinical care or post-marketing surveillance data to the country of concern pharmaceutical company. One commenter also asked that, if the Department did not categorically include these types of transactions within the scope of the rule, it clarify that the arrangement would be characterized as a vendor agreement that could proceed under § 202.401.

The Department does not assess that changes to the text of the exemptions are necessary. The exemption at § 202.510 permits U.S. persons to share certain bulk U.S. sensitive personal data with a country of concern or covered person, if doing so is ''necessary to obtain or maintain regulatory authorization or approval to research or market a drug, biological product, device, or combination product.'' The exemption is not limited to circumstances in which the data is necessary for the *U.S. person* to obtain or maintain regulatory authorization or approval to market a drug, biological product, device, or combination product. Accordingly, the Department intends for the exemption to cover arrangements in which a U.S. person shares ''regulatory approval data'' with a covered person, like a country of concern pharmaceutical company, if it would be necessary for the covered person to maintain regulatory authorization or approval to market the drug, biological product, device, or combination product, and the data transaction otherwise complies with the requirements of § 202.510.

The Department has also revised the text of § 202.510 to ensure that any such exempted data transactions apply to circumstances in which a person seeks approval or authorization to market or research a drug, biological product, device, or combination product in a third country that is not a country of concern. The NPRM limited the exemption to circumstances in which the exempted data transaction was necessary to ''obtain or maintain regulatory approval to research or market'' the covered products ''in a country of concern.'' However, the Department assesses that the humanitarian interest in enabling covered persons to market drugs, biological products, devices, and combination products in third countries

outweighs the risk of permitting U.S. persons to provide ''regulatory approval data'' to covered persons for the covered person to subsequently market a drug, biological product, device, or combination product either in the country of concern or in a third country.

The Department declines, however, to categorically exempt or characterize all such licensing transactions described by commenters without more information about the volume of such arrangements, the quantity and types of government-related data or bulk U.S. sensitive personal data U.S. companies provide to country of concern licensors, the extent to which such transactions would involve confidentiality protections to mask the identity of U.S. persons, and the value to U.S. patients and end-users of such products. Where the transaction does not fall into one of the existing exemptions, U.S. persons engaged in these types of licensing agreements may seek authorization for such transactions via a general or specific license, pursuant to subpart H, or an advisory opinion under subpart I.

Several commenters asked the Department to provide more specificity about what ''sensitive personal data'' the Department would consider ''reasonably necessary'' for a country of concern regulator to assess the safety and effectiveness of a drug, biological product, device, or combination product to satisfy the definition of ''regulatory approval data.'' The Department agrees with other commenters who encouraged the Department not to provide a brightline rule about what sensitive personal data would be ''reasonably necessary'' for a country of concern regulator to assess a product's safety and effectiveness because it would be difficult to anticipate all of the circumstances in which different types of sensitive personal data may be ''reasonably necessary'' to assess product safety and effectiveness in advance. Section 202.510 includes some examples of sensitive personal data the Department assesses would be ''reasonably necessary'' for a country of concern regulator to assess a product's safety or effectiveness. The Department welcomes U.S. persons to seek an advisory opinion about concrete data transactions they are anticipating pursuant to subpart I, or seek general or specific licenses to authorize data transactions they assess may be subject to subparts C and D, pursuant to subpart H, if more specificity is required.

One commenter expressed concern that the exemption would not apply to ''device[s],'' like certain medical technology products that provide treatment or diagnostic services, unless they relate to the treatment of diseases or directly affect the structure of a human body. The Department has incorporated the term ''device'' for the purposes of §§ 202.510 and 202.511, as that term is defined in 21 U.S.C. 321(h). That provision defines a ''device'' as, among other things, ''an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is—. . . (B) intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or (C) intended to affect the structure or any function of the body of man or other animals.'' The Department believes that the commenter may have misread the definition of ''device'' in 21 U.S.C. 321(h) as requiring that a ''device'' satisfy both subparts (B) and (C) of the definition, including each of the elements of subpart (B). The Department believes that the definition of ''device'' incorporated in §§ 202.510 and 202.511 likely would apply to many ''medical technology product[s]'' that are ''intended for use in the diagnosis of disease or other conditions.''

The same commenter encouraged the Department to add ''electronic products'' to the list of clinical investigations regulated by the FDA or supporting applications to the FDA for research or marketing permits for drugs, biological products, devices, combination products, or infant formula exempted from subparts C and D by § 202.511(a)(1). The commenter explained that its association members produce electronic products, like ultrasound imaging devices and blood warmers used for patient care, and that permitting these members to efficiently comply with international regulatory processes is essential to the members' competitiveness. As explained in part IV.D.7 of this preamble, § 202.511 incorporates the definition of ''device'' from 21 U.S.C. 321(h), which includes any ''instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article . . . intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals.'' Accordingly, the Department believes that the exemption in § 202.511(a)(2) may already apply to the ''electronic products,'' like ultrasound imaging devices and blood warmers, that the commenter explained were used in patient care for the ''diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease.'' The Department welcomes U.S. persons that produce ''electronic products'' outside the scope of the device definition incorporated by § 202.511 to provide more specific details about the data transactions related to their electronic products that the Department should consider exempting through a license to authorize such data transactions with a country of concern or covered person, pursuant to subpart H.

Some commenters requested that the Department add food products, including dietary supplements and ''health foods,'' and cosmetics to the lists of products in the exemptions in §§ 202.510 and 202.511. The commenters explained that, under some circumstances, countries of concern may require foreign producers of these products to submit data to country of concern regulators to obtain or maintain regulatory approval to market or research such products. The Department declines to adopt the commenters' recommendations. The exemptions in §§ 202.510 and 202.511 are tailored to balance the humanitarian interest in providing access to drugs, biological products, devices, and combination products to individuals in countries of concern and globally, and ensuring that manufacturers engaged in clinical trials and investigations of drugs, biological products, devices, combination products, or infant formula can collaborate internationally with the pressing national security risks described in the Order, NPRM, and this preamble about country of concern access to government-related data and bulk U.S. sensitive personal data.[165] The Department does not assess that the same humanitarian interests support exempting data transactions involving government-related data or bulk U.S. sensitive personal data relating to the production and marketing of dietary supplements or cosmetics in countries of concern from the prohibitions and restrictions in the rule, which are designed to mitigate the national security risk of country of concern access to such data. Further, commenters did not provide the Department with detailed enough information to assess whether the rule would impose meaningful restrictions on U.S. persons' ability to obtain or maintain regulatory approval to market or research dietary supplements or cosmetics in countries of concern. Regulated entities and persons may provide the Department more information about the specific data

[165] 89 FR 86118–19.

transactions that they assess the rule may affect and seek a license pursuant to subpart H.

One commenter recommended that the Department revise the definition of ''regulatory approval data'' to include submissions required by country of concern regulatory entities of bulk U.S. sensitive personal data—such as human genomic data or human biospecimens from which such human genomic data could be derived—to other covered persons—like a laboratory, institutional review board, or ethics committee in a country of concern—to obtain or maintain authorization to market a drug, biological product, device, or combination product. The Department agrees that data transactions that otherwise satisfy the definition of ''regulatory approval data'' and that are necessary to obtain or maintain authorization to market a drug, biological product, device, or combination product and that a country of concern regulatory entity requires a U.S. person to submit to another covered person for such purposes are exempt from subparts C and D. The Department has revised the exemption in § 202.510 accordingly.

Several commenters requested clarification about whether the term ''regulatory entity'' in § 202.510 includes local, municipal, provincial, and national regulators.

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 government-related data or bulk U.S. sensitive personal data directly to a government entity in a country of concern. Some commenters asserted that this would be unduly burdensome, but they did not provide any further information on the scope of that burden or the costs of compliance. One commenter asserted that the requirement was duplicative of some existing requirements or practices, suggesting that compliance will not be excessively costly even if it does require some changes to current practices. This commenter also sought further specificity on what records would be required to be kept under this section. Because of the variety of transactions that might occur, the Department does not believe it is feasible or appropriate to specify the precise records that must be maintained; the regulatory text requires a full and accurate record, which in many cases will likely include, at a minimum, the information set out in subparagraphs 4, 5, 6, 7, and 10 of § 202.1101(b).

Another commenter requested that recordkeeping and retention requirements not apply to U.S. companies engaging with third parties or vendors that assist in clinical and other research, unless those vendors ''have access to sensitive personal data that is not required for regulatory submission and is not de-identified,'' given that many countries of concern require by law that nationals of those countries provide certain data to regulatory authorities. This commenter added that because the Department is using the definition of ''personal health data'' from HIPAA, the de-identified ''regulatory approval data'' and ''clinical investigations and post-marketing surveillance data'' exempted at §§ 202.510 and 202.511 may be ''key-coded,'' as provided for at 45 CFR 164.514(c), as long as the key is not held by or accessible to a covered person, which will preserve essential product safety and post-marketing surveillance activities.

The Department declines to adopt the commenter's suggestions to eliminate the reporting requirements generally or for third-party vendors submitting regulatory approval data to a country of concern regulator specifically. The reporting and recordkeeping requirements required to comply with the exemptions at §§ 202.510 and 202.511 are essential for the Department to better understand the risk, if any, posed by sharing government-related data or bulk U.S. sensitive personal data with countries of concern or covered persons to obtain or maintain regulatory authorization to research or market products, or in the course of clinical investigations, product safety, or post-marketing product surveillance activities. Where country of concern law requires a U.S. company to engage a country of concern registered agent or vendor to submit such data, it is essential for the Department to have access to records and reporting involving the transactions between the registered agent or vendor and the country of concern regulators to weigh the risks, if any, posed by such transactions. Further, while entities invoking the exemptions under §§ 202.510 and 202.511 may maintain some records related to data collected about participants in their clinical trials, investigations, and post-marketing product surveillance activities to address potential patient privacy and informed consent concerns, the Department's recordkeeping and reporting obligations are driven by the Department's interest in better understanding the risk posed by sharing government-related data or bulk U.S. sensitive personal data with specific countries of concern or covered persons. The extant recordkeeping and reporting obligations imposed by other regulatory regimes do not address this national security risk-focused recordkeeping and reporting obligation.

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

In response to comments received at the ANPRM stage, the Department proposed an exemption related to clinical investigations and post-marketing surveillance data. Commenters were generally supportive of this exemption, although several commenters suggested that the exemption should be broadened in various ways. At a high level, these commenters expressed concern that, as proposed, the exemption might unduly harm biopharmaceutical innovation. One commenter, for example, emphasized that the rule, even with the exemption in § 202.511, might limit the pharmaceutical and medical device industry's access to organizations and individuals with valuable expertise and capabilities. The Department recognizes that a consequence of the rule—indeed, its purpose—will be to limit certain transactions with covered persons and countries of concern. But neither this commenter nor other commenters presented evidence that covered persons, as a class, possess unique capabilities that cannot be obtained from other sources. In such cases, a regulated person or entity could seek a specific license under § 202.802.

The Department has considered these comments and, as explained, has made some changes to or otherwise clarified the exemption. The Department believes that with these changes and clarifications, the exemption appropriately balances the need to mitigate the national security risk attendant to access to government-related data and bulk U.S. sensitive personal data against other interests, including humanitarian, economic, and scientific interests.

The Department believes that, as discussed in the NPRM,[166] existing FDA regulations governing clinical investigations and subject data offer sufficiently robust protection to at least mitigate national security concerns, and in light of the countervailing interests in allowing these types of transactions to proceed, the Department retains this

[166] *See* 89 FR 86138–40.

exemption, with some changes, in the final rule. Some commenters contended that the exemption should not be limited to FDA-regulated activities. For example, one commenter thought that the exemption should include ''local-for-local'' studies—that is, clinical trials conducted in a country of concern to support an application for approval by that country's regulators—even when the study is not regulated by the FDA. The Department believes that FDA regulations, though focused on a different problem, are essential to mitigate the national security risk identified in the Order, and declines to extend the exemption to non-FDA-regulated activities. The Department reiterates, however, that the rule does not restrict the transfer of non-U.S. person data to the United States and that many transactions can proceed as restricted transactions or subject to a license.

The Department proposed exempting transactions ''ordinarily incident to and part of'' either certain clinical investigations or certain post-market activities. The Department adheres in the final rule to that scope. One commenter suggested substantially broadening the exemption to reach transactions that are ''incidental to and in furtherance of'' such activities, to allow greater industry use of covered persons' expertise and capabilities. As explained, the Department recognizes that some transactions that might otherwise occur in the absence of the rule might not proceed, or might proceed only subject to the requirements for restricted transactions, without a broader exemption. But the Department has not seen evidence that covered persons possess irreplaceable expertise or capabilities, and it does not believe that the proposed change properly accounts for the national security concerns that arise from these types of transactions.

Other commenters sought clarification about whether the exemption would apply to entities involved in clinical research other than those actually performing the research, such as medical record companies or research ethics committees. The exemption is not limited to any particular type of entity, but rather is limited to those transactions that are ordinarily incident to and part of the specified activities. Entities seeking clarity about whether a particular transaction would fall within that exemption can avail themselves of the advisory opinion process set out in subpart I.

Some commenters recommended that the clinical investigations exemption apply to all transactions involved in clinical studies or investigations. The commenters did not provide adequate information about the types of transactions, the extent to which they would qualify as covered data transactions that involve access by a country of concern or covered person to government-related data or bulk U.S. sensitive personal data, or the necessity of such transactions for the Department to assess the risks and benefits of expanding the exemption. Notably, the Department revised the definition of ''covered data transaction'' in § 202.210 to clarify that the prohibitions and restrictions of the rule only apply to covered data transactions with a country of concern or covered person that involve access by a country of concern or covered person to government-related data or bulk U.S. sensitive personal data. The rule does not regulate transactions that do not implicate country of concern or covered person access to government-related data or bulk U.S. sensitive personal data. And the exemption for clinical investigations and certain clinical care and post-marketing surveillance data transactions already exempts any data transactions within the scope of the restrictions or prohibitions of subparts C and D, if they are ''ordinarily incident to and part of'' the relevant clinical investigations or collection and processing of clinical care or post-marketing surveillance data. The Department declines to specify in advance the types of data transactions that fall within the scope of the exemption and welcomes regulated persons or entities to seek an advisory opinion or apply for a license authorizing any such transactions that they assess fall within the scope of the rule's prohibitions and restrictions.

The Department does not intend to categorically preclude clinical investigations from being conducted in a country of concern and does not believe that the rule, even without the clinical investigation-focused exemption, does so. The rule generally does not prohibit or restrict data transactions from a country of concern to the United States and does not apply to data unrelated to U.S. persons. The Department sought 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. One commenter asserted that anonymized clinical data should be categorically exempted to avoid preventing companies from launching clinical trials in a country of concern, but they did not elaborate on how the rule, especially in light of the exemption for clinical investigations, would do so. The Department therefore rejects this suggestion.

Some commenters requested clarity about what standard for de-identification the Department intended to require for U.S. persons to avail themselves of the exemption. Consistent with many commenters' recommendations, the Department has adopted standards for de-identification or pseudonymization that are consistent with the FDA's practices for adverse event reporting in 21 CFR 314.80(i) for sensitive personal data implicated by §§ 202.510 and 202.511 and discussed in more detail in part IV.D.8 of this preamble.

The Department is also aware that, as appropriate and required, certain data related to post-marketing surveillance is made available to global public health authorities, such as the World Health Organization's Vigibase. Submissions by the United States Government itself, such as FDA submissions to Vigibase, would be exempt under § 202.504. Several commenters sought an explicit exemption for data repositories used to support medical and other public health research. These commenters expressed concern that, because covered persons or countries of concern might have access to bulk U.S. personal health or human genomic data submitted by a U.S. person, U.S. persons would not be permitted to submit data to these repositories. The Department declines to make any change. The rule's prohibitions and restrictions principally apply to covered data transactions between U.S. persons and covered persons or countries of concern. The rule's prohibitions and restrictions in subparts C and D typically would not apply, unless the data repositories to which U.S. researchers are submitting data are themselves covered persons. Further, such submissions of data may be exempt under § 202.507 or because the submission does not involve an exchange of money or other consideration to satisfy the definition of a covered data transaction. In cases where a regulated person or entity believes the operative provisions of this part otherwise apply, such as the provision requiring contractual limits on onward data transfers to countries of concern or covered persons in § 202.302, the Department encourages those parties to seek a license under subpart H. The available comments do not provide sufficient information for the Department to identify or describe the entities with whom transactions of this type should be exempted. But,

based on the public comments and subject to receipt of additional and more specific information, the Department believes it may be appropriate to issue general licenses that broadly authorize the submission of health- and medical research-related data to specific entities.

The Department sought comment on whether the FDA recordkeeping provisions in 21 CFR 312.62 would be adequate such that it would be unnecessary to also require compliance with the recordkeeping and reporting requirements set forth in §§ 202.1101(a) and 202.1102. After reviewing the comments on this subject, the Department makes no change in the final rule and does not seek to impose those requirements on entities availing themselves of this exemption.

The Department sought comment on 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. Some commenters expressed concern that the lack of clarity about the duration of the exemptions in §§ 202.510 and 202.511 would hinder U.S. companies' ability to research and market drugs, biological products, devices, and combination products. The Department agrees and has not imposed any expiration for the exemptions in the rule. As with any other provision of the rule, the Department may amend the rule in the future to address the national security risks posed by country of concern access to government-related data and bulk U.S. sensitive personal data.

The Department recognizes that some of the rule's prohibitions and restrictions may nonetheless affect some covered data transactions relating to clinical investigations and involving access by covered persons or countries of concern to government-related data or bulk U.S. sensitive personal data. The Department has established licensing provisions in subpart H to permit regulated persons or entities to seek the Department's authorization to continue otherwise regulated transactions. While some commenters valued the flexibility that licensing provides, they generally preferred the regulatory certainty of a regulatory exemption that could be supplemented by licenses for transactions outside the exemption. The Department agrees that this approach provides better clarity for regulated entities and will minimize, though not eliminate, disruption to medical research. The Department believes that both general and specific licenses will nonetheless play an important role in further mitigating disruption of medical research. One commenter, for example, suggested establishing a ''pathway'' for approving collaboration for specific research projects. The Department believes the existing licensing framework establishes just that pathway.

9. Exemptions for Non-Federally Funded Research

Several commenters expressed concerns that the rule would impede U.S. persons from participating in or sharing government-related data or bulk U.S. sensitive personal data pursuant to international research projects that involve countries of concern or covered persons, but that are not conducted pursuant to a contract, grant, or other agreement with the Federal Government or are not otherwise exempted by §§ 202.510 and 202.511. Commenters requested an exemption for such non-federally funded research. The Department declines to include an express exemption for non-federally funded research programs in the rule.

First, the definition of ''covered data transactions'' subject to the prohibitions and restrictions of subparts C and D identifies specific categories of data transactions to which the restrictions and prohibitions apply, each of which requires a commercial nexus. *See, e.g.,* § 202.214 (defining ''data brokerage'' as ''the sale of data, licensing of access to data, or similar commercial transactions involving the transfer of data''), § 202.217 (defining ''employment agreement'' as ''any agreement or arrangement in which an individual . . . performs work or job functions directly for a person in exchange for payment or other consideration''), § 202.228 (defining ''investment agreement'' as ''an agreement or arrangement in which any person, in exchange for payment or other consideration, obtains direct or indirect ownership interests or rights in relation to'' property or entities), § 202.258 (defining ''vendor agreement'' as ''any agreement or arrangement . . . in which any person provides goods or services to another person . . . in exchange for payment or other consideration''). Commenters did not provide adequate information for the Department to assess whether the non-federally funded research about which they raised concerns would satisfy the nexus to a commercial transaction required by the specified categories of covered data transactions. To the extent that U.S. persons' non-federally funded research would involve access to government-related data or bulk U.S. sensitive personal data by a country of concern or covered person and one of the specified categories of covered data transactions involving a payment or other consideration, the Department would welcome such regulated persons or entities to provide additional information necessary for the Department to assess the risks and benefits of the proposed transactions and apply for a specific license to authorize any such data transactions.

Second, the rule does not impose any restrictions on U.S. persons accessing government-related data or bulk U.S. sensitive personal data. To the extent that commenters are concerned that the rule would directly impede their participation in non-federally funded research involving their access to government-related data or bulk U.S. sensitive personal data, the rule is limited to restricting or prohibiting certain covered data transactions involving access by countries of concern or covered persons to government-related data or bulk U.S. sensitive personal data.

Third, the rule does not regulate any publicly accessible material, including data that would otherwise constitute government-related data or bulk U.S. sensitive personal data in open-access data repositories. Commenters expressed concern that the rule would impede their ability to engage in research involving open-access data repositories. The definition of ''sensitive personal data'' excludes any data that is, at the time of the transaction, lawfully available to the public from a Federal, State, or local government record or in widely distributed media, including unrestricted and open-access data repositories. Similarly, the exemption for data transactions conducted pursuant to a contract, grant, or other agreement with a Federal agency or department would exempt from the prohibitions and restrictions of subparts C and D the sharing of data with an open-access data repository authorized by contract, grant, or other agreement with the Federal agency or department.

Fourth, the Department exempted certain clinical investigations regulated by the FDA in § 202.511(a)(1) because the Department agrees that the protections involving clinical investigation participants' data and the humanitarian interests in promoting the development of new drugs, biological products, devices, and combination products to diagnose, treat, and prevent disease and other medical conditions, and infant formula outweigh the national security risks of countries of concern obtaining access to government-related data or bulk U.S. sensitive personal data. Similarly, the Department exempted research conducted pursuant to a grant, contract, or other agreement

with the Federal government in § 202.504 because Federal agencies may impose contract, grant, or agreement-based restrictions and reporting requirements on U.S. persons to protect government-related data and bulk U.S. sensitive personal data from exploitation by countries of concern.[167]

Non-federally funded research activities and research activities outside the scope of clinical investigations regulated by the FDA do not provide the same federally imposed protections and reporting requirements on government-related data or bulk U.S. sensitive personal data necessary to mitigate and better assess the risks of country of concern access to government-related data or bulk U.S. sensitive personal data involved in such research activities.

Fifth, at least one commenter explained that there may be circumstances in which clinical trials or emergency care situations supported by private foundations or non-governmental organizations involve the transfer of biological products that the commenter assessed could violate the prohibition on transfers of bulk human 'omic data and biospecimens from which such data could be derived. The exemption in § 202.511 exempts certain data transactions involving clinical investigations regulated by the FDA or required for applications to the FDA for research or marketing permits for drugs, biological products, devices, combination products, and infant formula, and data transactions ordinarily incident to and part of the collection and processing of clinical care data or post-marketing surveillance data necessary to support or maintain authorization by the FDA, regardless of whether the entity engaged in the clinical investigation receives Federal funding. And the Department has revised the definition of ''human biospecimens'' in § 202.223 to exclude human biospecimens intended by a recipient solely for use in diagnosing, treating, or preventing any disease or medical condition.

In light of these considerations, the Department declines to provide a general exemption for non-federally funded research at this time. To the extent that U.S. persons are concerned that they are involved in covered data transactions involving access by countries of concern or covered persons to government-related data or bulk U.S. sensitive personal data in the course of their non-federally funded research activities, they may seek a general or specific license authorizing those data transactions, pursuant to subpart H.

[167] *See, e.g.,* 89 FR 15426.

E. Subpart F—Determination of Countries of Concern

1. Section 202.601—Determination of Countries of Concern

In the proposed rule, the Attorney General 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. sensitive personal data to the detriment of the national security of the United States or the security and safety of U.S. persons.

One commenter expressed support for the designated countries of concern and for the fact that the Department made country of concern determinations based on the countries' specific actions. According to the commenter, this approach would allow the Department to remove or add countries to and from the list of countries of concern depending on their conduct. The Department agrees and notes that, with the concurrences of the Secretaries of State and Commerce, it has the authority to amend the list of countries of concern. In doing so, the Department would undertake a rulemaking that is subject to the ordinary process of robust interagency review and notice and public comment.

One commenter asserted that the proposed rule's restrictions on data transactions to China and other countries are discriminatory and violate international law, the United Nations Charter, and World Trade Organization economic and trade rules. The commenter expressed firm opposition to the rule, demanded that the Federal Government stop what it characterized as discriminatory treatment of China, and reserved its right to pursue countermeasures.

The rule's restrictions are not discriminatory; they are based on countries engaging 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 posing 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 the security and safety of U.S. persons. The countries of concern have engaged in years of adverse and continuing conduct that the Department set forth in detail in the NPRM[168] and in parts III, IV.B, IV.C and IV.E of this preamble.[169]

Even just between issuance of the NPRM and the final rule, new incidents have come to light that demonstrate how China continues to aggressively threaten U.S. national security. For example, according to a recent press release issued jointly by the Federal Bureau of Investigation and CISA, ''PRC-affiliated actors have compromised networks at multiple telecommunications companies to enable the theft of customer call records data,'' and ''the compromise of private communications of a limited number of individuals who are primarily involved in government or political activity.'' [170]

There have also been numerous recent examples of U.S. persons acting as unregistered agents of China. For example, in August 2024, a U.S. person pled guilty after obtaining a wide variety of information at the request of Chinese intelligence, including information about Chinese dissidents and pro-democracy advocates, members of the Falun Gong religious movement, and his employer, a major U.S. telecommunications company.[171] In September 2024, a Federal grand jury returned an indictment charging a former New York State government employee for acting as an undisclosed agent of the Chinese Government and the CCP. In exchange for substantial economic and other benefits, this individual wielded influence among State executives and engaged in political activities that served the interests of the PRC and Chinese Communist Party, such as changing high-level New York State officers' messaging regarding issues of importance to the PRC and Chinese Communist Party and blocking representatives of the Taiwanese

[168] 89 FR 86141–44.

[169] 89 FR 86140–48.

[170] Press Release, CISA, *Joint Statement From FBI and CISA on the People's Republic of China (PRC) Targeting of Commercial Telecommunications Infrastructure* (Nov. 13, 2024) *https://www.cisa.gov/news-events/news/joint-statement-fbi-and-cisa-peoples-republic-china-prc-targeting-commercial-telecommunications* [*https://perma.cc/DX86-WM6Y*].

[171] *See, e.g.,* Plea Agreement, *United States* v. *Ping Li, supra* note 113.

government from having access to high-level New York State officers.[172]

Moreover, the commenter does not cite any specific provisions of international agreements that it alleges the rule would violate, making it difficult for the Department to fulsomely respond to the comment. Nevertheless, as the Department discussed in further detail in the NPRM and part IV.D.5 of this preamble, the rule's prohibitions and restrictions on access to government-related data and bulk U.S. sensitive personal data by countries of concern are consistent with or otherwise permissible under trade and other international agreements, including for example, pursuant to the security exception to the World Trade Organization's General Agreement on Trade in Services.[173]

Finally, because it is outside the scope of the rule, the Department does not respond to the commenter's threat to take retaliatory measures in response to the rule.

F. Subpart G—Covered Persons

1. Section 202.211—Covered Person

The proposed rule identified a ''covered person'' as an individual or entity that falls into one of four classes of covered persons, or that the Attorney General has designated as a covered person. The NPRM noted that an entity is automatically 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. As the NPRM also explained, 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.[174] The NPRM noted that any foreign person that is an individual is also a covered person if that individual is an employee or a contractor of a country of concern or of a covered person that is an entity;[175] or if that individual is primarily a resident in the territorial jurisdiction of a country of concern is also a covered person.[176] Lastly, the NRPM listed criteria governing the Department's designation of covered persons.[177]

The Department has slightly amended the language of §§ 202.211(a)(1) and (2) to now apply to (1) a foreign person that is an entity that is 50 percent or more owned, directly or indirectly, individually or in the aggregate, by one or more countries of concern or persons described in § 202.211(a)(2); or that is organized or chartered under the laws of, or has its principal place of business in, a country of concern; and (2) a foreign person that is an entity that is 50 percent or more owned, directly or indirectly, individually or in the aggregate, by one or more persons described in §§ 202.211(a)(1), (3), (4), or (5).

These technical corrections, which do not alter the intended scope of the criteria for covered persons, were necessary for three reasons. First, the Department streamlined the language in § 202.211(a)(2) that references subsections of the covered person criteria for the sake of clarity and concision. Second, the Department changed the 50-percent rule language in §§ 202.211(a)(1) and (2) to more closely match OFAC's 50-percent rule language, because the Department intends for the rules to generally be applied in a similar manner. This corrected language will capture, as was originally intended, indirect ownership as it relates to certain complex ownership structures—such as where two covered persons each own minority stakes in a subsidiary, but their aggregate ownership meets or exceeds the 50-percent threshold—consistent with OFAC's implementation of the 50-percent rule.

Third, the Department added ''or persons described in § 202.211(a)(2) of this section'' to ensure that foreign persons that are entities and 50 percent or more owned by a covered person are in scope. Again, this technical correction is not an expansion of the intended scope of this category of covered persons. Instead, this correction aligns the category with the description in the NPRM, which says, ''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.''[178] This therefore does not present a substantive change in the scope as proposed in the NPRM.[179]

One commenter suggested that the Department refine the covered person definition to avoid under inclusion and overinclusion. The commenter noted that an entity that is 50 percent owned by a country of concern presents the same risk as an entity with 49 percent ownership, even though the latter would not automatically be considered a covered person. The commenter is correct that an entity that is controlled, but not 50 percent or more owned, by one or more covered persons or countries of concern is not categorically considered a covered person under § 202.211(a). At this time, however, the Department does not believe that a significant minority interest necessarily presents the same level of risk as a majority interest such that the 50-percent rule should be lowered, and other considerations—including the need for an objective, brightline rule and industry's experience in complying with the 50-percent rule in other national security contexts—justify adherence to the 50-percent rule.

The Department agrees, however, that a controlling interest may present risks of access, which is why control is one of the criteria for the Department to designate an entity as a covered person under § 202.211(a)(5) if such an entity is determined to meet the relevant criteria. U.S. persons should exercise caution when considering engaging in covered data transactions with an entity that is not a covered person but in which one or more covered persons have significant ownership that is less than 50 percent, or which one or more covered persons may control by means other than a majority ownership interest. Ownership percentages can fluctuate such that an entity could become a covered person, and such entities may be designated by the Department based on the significant controlling interest. Additionally, persons should be cautious in dealing with such an entity to ensure that they are not engaging in evasion or avoidance of the regulations.

One commenter recommended that the Department consider applying the knowledge-based standard currently employed by BIS export control rules, which prohibits U.S. persons from proceeding with a transaction if they have actual knowledge that a violation of the Export Administration Regulations has occurred or is about to occur. As justification, the commenter explained that companies that meet the covered person criteria based on their 50 percent ownership may not be publicly traded, or they may be small businesses and startups invested in by larger entities whose own ownerships may shift with market conditions. The comment provides no analysis for whether the BIS knowledge standard would adequately address the national security concern as compared to the

[172] Press Release, U.S. Dep't of Just., *Former High-Ranking New York State Government Employee Charged with Acting as an Undisclosed Agent of the People's Republic of China and the Chinese Communist Party* (Sept. 3, 2024), *https://www.justice.gov/usao-edny/pr/former-high-ranking-new-york-state-government-employee-charged-acting-undisclosed* [*https://perma.cc/M2A8-FDGC*].

[173] 89 FR 86120.

[174] 89 FR 86148.

[175] *Id.*

[176] *Id.*

[177] 89 FR 86150–51.

[178] 89 FR 86148.

[179] 89 FR 86148–50.

''knowingly'' standard that the rule already adopts.

Relatedly, another commenter suggested modifying the rule to allow U.S. persons to rely on certifications and supporting documentation provided by persons to establish their status as non-covered persons. This commenter asserted that research institutions are not sophisticated or capable enough to run compliance programs.

The Department declines to make any changes to the rule in response to the above comments. The regulations do not prescribe or endorse any specific method to screen counterparties to determine their status as covered persons. Consistent with the NPRM, U.S. persons should employ compliance programs that are based on their ''individualized risk profile . . . [which may] 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.'' [180] Additionally, the rule's prohibitions and restrictions are subject to a knowingly standard, which generally mitigates the commenters' concerns. In many circumstances, depending on a U.S. person's individualized risk profile, a party's own statements or the records maintained by third parties may be an appropriate part of a compliance program to confirm the covered person status of counterparties.

One commenter suggested that the Department aid business compliance efforts and automated due diligence by making the Covered Persons List ''as comprehensive as possible'' by regularly updating and including aliases and technical identifiers. Another commenter similarly requested that the Department provide legal certainty and ease compliance by taking an approach under which transactions with listed entities are prohibited. The commenter noted that the Cyberspace Administration of China has ordered that access to databases listing corporate entities and corporate ownership structures be discontinued for non-Chinese database users. As a result, the commenter noted that it may prove difficult for U.S. companies—particularly small- and medium-sized U.S. businesses, which the commenter noted make up more than 90 percent of the manufacturing industry—to ascertain whether an entity is within the scope of § 202.211(a).

As discussed in part IV.E of the NPRM's preamble, the Covered Persons List will include each covered person that is designated by the Department.[181] While these comments do not necessitate any change to the rule, the Department will endeavor to provide sufficient details about designated persons to aid the private sector in its compliance efforts associated with identifying and screening designated covered persons. The Department also supports automating and streamlining compliance and intends to pursue this suggestion as part of publicly maintaining the Covered Persons List, such as by offering text and PDF versions of the Covered Persons List for manual review, and data file versions of the list that could be designed to facilitate automated screening. Depending on a U.S. person's scale, sophistication, and risk profile of their business, it may be appropriate for a U.S. person to consider using one of the numerous commercially available screening software packages as part of a compliance program.

The Covered Persons List, however, will not exhaustively identify all covered persons. Monitoring compliance against a non-exhaustive list is not novel to the regulated public that engages in cross-border transactions. Indeed, maintaining a non-exhaustive list is consistent with the practice at OFAC, which maintains several non-exhaustive sanctions lists, including the Specially Designated National and Blocked Persons List (''SDN list'') and the Sectoral Sanctions Identifications List. U.S. persons engaging in covered data transactions may likely already screen cross-border transactions and other dealings against the OFAC SDN list. As OFAC notes in its Frequently Asked Question #91, ''some OFAC sanctions block categories of persons even if those persons do not appear in the SDN list, including . . . persons blocked pursuant to OFAC's '50 Percent Rule' . . . . The property and interests in property of such an entity are blocked regardless of whether the entity itself is listed on the SDN list.'' [182] As indicated in the ANPRM and NPRM, the private sector will need to screen their transaction counterparties, vendors, employers, and investors to determine whether they meet the categories of covered persons in § 202.211(a), in addition to those on the Covered Persons List.[183] U.S. persons who comply with OFAC sanctions should be familiar with taking a risk-based approach to sanctions screening such that this concept will not be novel.

A commenter argued that it is often nearly impossible, from a compliance perspective, for companies to determine ownership of companies located in a country of concern. This comment was entirely conclusory, and the Department disagrees. U.S. persons (and persons otherwise subject to U.S. jurisdiction) already must ensure that they are not engaging in trade or other transactions with persons designated by OFAC.[184] The commenter is silent on the specific ways in which the Department's rule requiring due diligence into company ownership would be harder to comply with than OFAC's regulations, which also expect the regulated community to screen for ownership. OFAC's 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 SDN list.[185] As such, the Department expects that much of the regulated public will have already have experience developing and implementing a tailored, risk-based compliance program for sanctions screening that includes methods for determining whether a foreign vendor, contractor, or counterparty is an SDN or owned by an SDN. The Department declines to make any change to the rule in response to this comment.

Several commenters asserted that the categories of covered persons are too broad. These comments, however, are generally premised on various misapplications of the categories. For

[180] 89 FR 86152–53.

[181] 89 FR 86150–51.

[182] Off. of Foreign Asset Control, U.S. Dep't of Treas., *Frequently Asked Questions: 91. What Lists Does OFAC Maintain? Where Can I Find These Lists?* (Aug. 21, 2024), *https://ofac.treasury.gov/faqs/91* [*https://perma.cc/Q8XA-RJ2Z*].

[183] 89 FR 86149–51.

[184] *See, e.g.,* Off. of Foreign Asset Control, U.S. Dep't of Treas., *Frequently Asked Questions: 65. How Frequently Is an Insurer Expected to Screen Its Databases for OFAC Compliance?* (Nov. 13, 2024), *https://ofac.treasury.gov/faqs/65* [*https://perma.cc/VJM5-DTXD*]; Off. of Foreign Asset Control, U.S. Dep't of Treas., *Frequently Asked Questions: 95. Does a Financial Institution Have the Obligation to Screen Account Beneficiaries for Compliance With OFAC Regulations?* (Dec. 4, 2006), *https://ofac.treasury.gov/faqs/95* [*https://perma.cc/RXN9-YXZU*]; Off. of Foreign Asset Control, U.S. Dep't of Treas., *Frequently Asked Questions: 445. What Are My Compliance Obligations With Respect to E.O. 13694, as Amended?* (Dec. 29, 2016), *https://ofac.treasury.gov/faqs/445* [*https://perma.cc/C5RP-GGN4*]; Off. of Foreign Asset Control U.S. Dep't of Treas., *Frequently Asked Questions: 813. As a Member of the Art Community, What Are My Compliance Obligations With Respect to Executive Order 13224, as Amended?* (Dec. 13, 2019), *https://ofac.treasury.gov/faqs/813* [*https://perma.cc/RUW8-VMK4*].

[185] *See generally* Off. of Foreign Asset Control, 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*].

example, one commenter noted a concern that a company's ''association with a country of concern'' would restrict that company from receiving data from U.S. companies. The commenter further noted that this concern is especially salient for entities on the Covered Persons List that are owned by a country of concern or an entity located in those countries. But a company does not become a covered person merely for having ''an association'' with a country of concern or a covered person. As listed in § 202.211(a), the criteria for falling into a covered person category or for being designated as a covered person are more rigorous than merely having associated with a country of concern or covered person. The scope of the categories of covered persons is correlated to the risk that a person or entity could be leveraged by a country of concern for access to government-related data or bulk U.S. sensitive personal data. A company merely being ''associated'' with a country of concern or covered person, absent a reason to believe they meet § 202.211(a) criteria, does not rise to the level of risk that the rule intends to address and is an exaggeration of the rule's prohibitions.

As another example, another commenter claimed that there are 40 million ''registered'' firms in one of the countries of concern and asserted that all of them would be considered covered persons under the rule. Section 202.211(a) does not categorically treat an entity as a covered person just because it is ''registered'' in a country of concern. Instead, it covers foreign person entities that are ''organized or chartered under the laws of'' or have their ''principal place of business in'' a country of concern. Registration to do business in a country is legally different than being organized under the laws of a country or having a principal place of business there. The latter is far narrower in scope than those merely ''registered in'' a country of concern, which could include, for example, companies that do no business in a country, or those that are not subject to the direction or control of its government, but register in order to protect their intellectual property.

Additionally, the rule does not require U.S. persons to identify and catalogue every individual and entity that meets the covered person criteria. Instead, the rule requires U.S. persons to examine their much smaller demographic of current or prospective clients, vendors, employees, and investors to determine whether those individuals or entities meet the criteria of § 202.211(a). This commenter has chosen to mis-frame the rule as if it requires a U.S. person to boil the ocean (identify every covered person in the world), when it merely requires a U.S. person to boil their own pot (know their own customers, vendors, employees, and investors).

The same commenter stated that every single vendor, employment, and investment agreement with these ''registered'' entities would be subject to the Department's rule. Again, this comment misapplies the rule, artificially inflating its scope. The commenter neglects to consider any of the other elements or scoping of the rule. Other than the limited onward-transfer provision, the rule regulates only enumerated types of commercial transactions by U.S. persons with countries of concern or covered persons that give those countries or covered persons access to government-related data or to the six types of bulk U.S. sensitive personal data that meet or exceed the bulk thresholds, where none of the exemptions, general licenses, or specific licenses apply. This comment also neglects to consider that the rule does not prohibit the restricted transactions but rather allows U.S. persons to engage in such transactions under the condition that they comply with certain security and other requirements.

Another commenter expressed concerns that some may misinterpret the rule as prohibiting U.S. persons from allowing foreign researchers of a country of concern nationality access to Americans' data. As such, the commenter requested clarification of whether foreign researchers working for companies outside of countries of concern are excluded from the rule's provisions even if such foreign researchers are of a country of concern nationality.

Under the rule's definition of a covered person, a foreign individual (such as a researcher) who is a national of a country of concern would not be a covered person unless they (1) primarily reside in a country of concern; (2) are employed by or a contractor of a country of concern or a covered person; or (3) are designated by the Department as a covered person.

As the Order and rule make clear, the definition of ''covered person'' follows risk, not race, nationality, or ethnicity. The Order and rule are directed at persons of any race, nationality, or ethnicity 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. The rule does not categorically treat country of concern nationals that are 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, the rule treats only a subset of country of concern nationals 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. 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 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, any U.S. citizen or lawful permanent resident, and any person who has been granted asylum or refugee status in the United States. For example, under the 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 race, nationality, or ethnicity 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 rule adopts the approach described in the NPRM without change.[186]

[186] 89 FR 86150.

One commenter asked for clarification on when a foreign company is ''in the United States'' with respect to the definition of ''U.S. person'' in § 202.256. More specifically, the commenter asked whether a company that conducts business with U.S. individuals but does not have a U.S. branch or subsidiary could meet the definition. Selling to U.S. customers does not place a foreign person ''in the United States.'' A foreign company with no headquarters, subsidiary, or other physical presence in the United States is not ''in the United States'' for the purposes of § 202.256.

One commenter asserted that the proposed rule's definitions of covered person, person, foreign person, and U.S. person are internally inconsistent because the proposed rule treats Chinese or Russian citizens located in the United States as U.S. persons, but it treats U.S. branches of companies organized under the laws of a country of concern as foreign persons. The commenter asked that the Department ensure that the definitions align and treat entities and individuals alike, or that the Department modify the definitions to demonstrate how entities and individuals are treated differently.

The proposed rule does not treat entities and individuals differently; rather, it treats branches of companies, which are not independent entities and do not have their own separate corporate personhood, as part of their parent companies. As a result, as demonstrated in the examples at §§ 202.256(b)(7) and (8), the U.S. branch of a company organized under the laws of a country of concern is treated as a foreign person, but a U.S. subsidiary of a foreign company, which is a separate entity from the parent, is treated as a U.S. person. This treatment of foreign branches aligns with OFAC's treatment of foreign branches in its IEEPA-based sanctions programs. The Department has added related examples in §§ 202.211(b)(7) and (8) to further illustrate this point.

One commenter listed several fact patterns involving U.S. person entities that were owned 50 percent or more by covered persons or countries of concern and noted that these U.S. person entities ''would be covered persons'' under the rule. As described in the ANPRM, including its Example 33, anyone in the United States (including those 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.[187] *See also* Example 6 in § 202.211(b)(6). Furthermore, the categories of covered persons in §§ 202.211(a)(1) through (4) explicitly apply only to foreign persons, not U.S. persons, and the category in § 202.211(a)(5) (which applies to any person) requires individual designation by the Department. The rule does not treat any U.S. person, including a U.S. subsidiary of a covered person, as a covered person unless the Department has individually designated the U.S. person as a covered person. The rule adopts the NPRM's examples illustrating the differences in treatment between a U.S. subsidiary and its foreign owner, as well as between U.S. companies and their foreign branches. The rule adopts this proposal unchanged from the NPRM.

The same commenter also provided several scenarios involving entities that the commenter concluded would meet covered person criteria in §§ 202.211(a)(2) or (3). In these examples, the commenter repeated essentially the same fact pattern: A country of concern owns 50 percent of third-country Company A that, in turn owns 50 percent of a second third-country Company B. In some instances, the commenter stated that Company B would be a covered person under the rule because of the country of concern's mere 25 percent indirect ownership.

This reasoning misapplies the 50-percent rule. Company B is a covered person, but not because the country of concern indirectly owns 25 percent of the company. Twenty-five percent ownership by a country of concern or covered person is less than the 50-percent rule requires. Instead, Company B is a covered person because it is 50 percent or more owned by a covered person (Company A), and Company A is a covered person because it is 50 percent or more owned by a country of concern. If, however, Company A were not a covered person (because its country of concern ownership was less than 50 percent and it did not meet any other criteria for covered persons), then Company B would not be a covered person, even with its less-than-50-percent indirect ownership by a country of concern. The Department has added an example at § 202.211(b)(8) to further clarify this point.

The commenter recited several additional scenarios that can be reduced to the same fact pattern described above, each referring to subsidiaries located in different countries that are not countries of concern. The commenter's examples mention various non-country of concern locations where countries of concern and covered persons may have set up subsidiaries, and asserts that the existence of these subsidiaries somehow makes the rule overbroad. The commenter appears to be claiming that a rule that targets a country of concern or covered person should regulate only persons and property within that country's territory, and that any other result is evidence of the rule's overbreadth.

The Department disagrees and is not aware of any precedent for such a claim. The fact pattern discussed above and the examples in the rule are classic demonstrations of the 50-percent rule being applied as intended. The commenter does not explain how the application of the 50-percent rule, which is drafted to match the longstanding language and application used by OFAC for years, somehow produces an unexpected or overbroad result.

In the sanctions' context, for example, if OFAC designates and blocks a Russian bank that operates in Russia and is owned by Russian government, all property and interests in property of that Russian bank are also blocked by operation of law. If that Russian bank operates subsidiaries in countries outside of Russia, even in countries that are partners and allies of the United States, those subsidiaries would be blocked persons by operation of law and U.S. persons would be prohibited from engaging in transactions and dealings with those subsidiaries, wherever located, unless exempt or otherwise authorized. The commenter provides no justification or argument explaining why consistent application of the 50-percent rule across regulatory programs would be inappropriate in the context of this rule.

In addition, the cross-border nature of countries of concern and covered persons' corporate hierarchy further supports the need for the rule to regulate covered persons that are outside a country of concern. Specifically, the national security and foreign policy risks identified in the Order exist 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 countries of concern listed in the rule have legal or political systems that allow those countries to obtain sensitive personal data (and access to such data) from persons subject to a country of concern's ownership, direction, jurisdiction, or control without due process or judicial redress.[188] Those risks exist with

[187] 89 FR 15790–91.

[188] Nat'l Counterintel. & Sec. Ctr., *supra* note 67, at 1; Justin Sherman, *Russia Is Weaponizing Its*

Continued

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. According to the FBI, ''[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.'' [189] For example, DHS explained in 2020 that ''PRC laws are most effective at creating compulsory data access when the data travels through a PRC firm abroad or a firm located within the PRC.'' [190] The categories of covered persons defined in the Order and defined further in the rule identify categories of persons that present such hybrid commercial threats because they are meaningfully subject to the ownership, direction, jurisdiction of a country of concern, or to the control of a country of concern or covered person.

One commenter requested, in the context of restricted transactions, that the Department limit the definition of ''covered person'' to the criteria listed in §§ 202.211(a)(1), (4), and (5). According to the commenter, for foreign persons meeting the criteria in §§ 202.211(a)(2) through (3), the nexus to a country of concern is weak and it would be too difficult for businesses to assert controls across all restricted transactions. The commenter provided the following example: A Japanese national (or a national of a country that is not a country of concern) owns Company A, which is incorporated under the laws of China. Company A owns 50 percent or more of Company B, an Australian company, and Company B hires a contractor who is a Canadian national. The commenter asserts that scenarios where a U.S. person engages in a restricted covered data transaction involving a vendor agreement with the contractor pose only a highly attenuated national security risk.

The Department disagrees. Company B's majority ownership by Company A—which carries with it formal control over all business decisions, a controlling level of informal influence, and a formal legal jurisdiction over Company B—is a classic example of a hybrid commercial threat. Any work completed by the contractor, who meets the covered person category in § 202.211(a)(3), carries this same risk. The commenter's scenario highlights the pervasiveness of the threat, as well as the reach that countries of concern have to try to obtain access to Americans' data. The scenario indeed reinforces that, without engaging in robust due diligence, U.S. companies could unknowingly provide foreign adversaries with the means to access data that harms America's national security. As such, the rule adopts the approach described in the NPRM without change.

Finally, one commenter suggested that the Department exempt from the prohibitions of the rule any covered persons who are ethical and compliant to prevent undue restrictions on legitimate research. The Department declines to adopt this suggestion. As explained in the NPRM, countries of concern have the legal authority or political systems to force, coerce, or influence persons under their jurisdiction to share their data and access with the country of concern's government, regardless of how ethical or trustworthy the person is.[191]

2. Section 202.701—Designation of Covered Persons

The proposed rule provided 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, except as otherwise authorized under the rule. As set out in the NPRM, this process is modeled generally on the processes for designation under the various sanctions' lists maintained by OFAC. The Department received only limited comments on this subject, and it adopts the proposed regulation without change.

One commenter suggested that the criteria for designation as a covered person were insufficiently determinate and that U.S. persons would avoid legitimate transactions for fear that their counterparties might be designated at some point in the future. The Department believes this concern is too speculative to support a change in the designation criteria, which themselves reflect the criteria established by the President in the Order. Although resource and information constraints or other factors will require the Department to exercise a degree of discretion in choosing which potentially designable persons should be pursued for designation, whether a person is subject to designation is reasonably determinate once relevant facts are known. As in the context of analogous sanctions regimes, U.S. companies routinely perform due diligence on prospective counterparties. That U.S. persons may lack access to the same information that the Department has in assessing their potential counterparties' risk for designation is unavoidable and does not warrant changing the criteria. Moreover, § 202.901 establishes a process for seeking an advisory opinion from the Department on contemplated transactions.

The same commenter suggested that the rule exempt from designation U.S.-based subsidiaries that adopt the CISA security requirements and U.S.-based subsidiaries that have a substantial presence in the United States. This commenter, as well as another

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, *2022 Country Reports on Human Rights Practices: Venezuela* 19 (2022), *https://www.state.gov/wp-content/uploads/2023/02/415610_VENEZUELA-2022-HUMAN-RIGHTS-REPORT.pdf* [*https://perma.cc/7TM9-P87S*]. *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*]; U.S. Dep't of Homeland Sec., *supra* note 57; 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. &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, C6, *https://freedomhouse.org/country/iran/freedom-net/2024* [*https://perma.cc/2QKR-9E7C*].

[189] *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).

[190] U.S. Dep't of Homeland Sec., *supra* note 57, at 10.

[191] 89 FR 86148–50.

commenter, also observed that entities—such as U.S. subsidiaries of covered person-owned companies—may be unable to take actions to avoid designation. The Department rejects these suggestions. As explained in the NPRM, the designation process allows the Department to address risks to national security that may arise from the designated person's relationship—whether voluntary or involuntary—with a country of concern.[192] As a general matter, the national security risk from concluding a covered data transaction with such a person may arise from the potential actions of the government of the country of concern in relation to that person, and not necessarily from the intent or personal characteristics of the individual or entity. The scope of a subsidiary's business in the United States or its adoption of security measures may be relevant to the exercise of the Department's discretion to designate that subsidiary but will not categorically exempt the subsidiary from designation. Under the final rule, an entity whose relationship with a covered person or country of concern changes—for example, through divestment by the covered person owner—such that the entity would no longer be subject to ownership or control by a covered person or otherwise satisfy the designation criteria, would be able to seek removal from the Covered Persons List.

Two commenters raised identical concerns that designations would not be subject to independent judicial review. A designated person or entity can petition the Department directly for reconsideration of its designation, and the Department also anticipates that designated entities will be able to avail themselves of existing judicial remedies, including, as applicable, under the Administrative Procedure Act, 5 U.S.C. 701 *et seq.* These commenters also objected that consultation by the Department with other agencies when making designation decisions was not mandatory. The commenters do not explain how mandatory consultation in every instance would meaningfully improve the rule, and the Department believes that mandatory consultation would unduly hinder administration of the rule by slowing decision-making and by needlessly diverting other agencies' resources from their primary missions. For example, it may be unnecessary to consult with the Department of Health and Human Services when contemplating a designation of an entity that works in the financial sector. The Department does expect to consult the Department of State on foreign policy concerns and other agencies as appropriate based on their applicable equities and expertise. The final rule better reflects this intention by explicitly including the Department of State in the list of agencies to be consulted. These commenters also objected to the use of classified information in designation decisions. However, use of classified information is expressly contemplated by IEEPA, *see* 50 U.S.C. 1702(c), and courts have routinely upheld the use of classified information in the IEEPA context. *See, e.g., Global Relief Found., Inc.,* v. *O'Neill,* 315 F.3d 748, 754 (7th Cir. 2002); *cf. People's Mojahedin Org. of Iran* v. *Dep't of State,* 327 F.3d 1238, 1242 (D.C. Cir. 2003).

Another commenter raised concerns that the designation process would violate due process in some circumstances. Although the Department believes that due process concerns are best addressed in the context of a specific case, it is confident that the process outlined—which largely mirrors the process used by OFAC for designating sanctions targets—is consistent with the Constitution and due process principles. Due process is a flexible concept, and the Constitution's preference for pre-deprivation notice and opportunity to be heard is subject to many exceptions, including when, as here, a pre-deprivation notice and hearing would risk the very harm to public interest that the government seeks to limit. *See, e.g., Gilbert* v. *Homar,* 520 U.S. 924, 930 (1997) (suspension without pay of State employee); *FDIC* v. *Mallen,* 486 U.S. 230, 240 (1988) (suspension of banking license). As explained in the NPRM, designations must be immediately effective to prevent designated covered persons from engaging in transactions that create the national security risk that the designation is designed to avoid; the data, once transferred to the jurisdiction of a country of concern, likely cannot be clawed back.[193] Pre-deprivation notice would create the same risk, and in these circumstances the flexibility of due process principles permits the government to rely on post-deprivation process. *See Glob. Relief Found.,* 315 F.3d at 754; *Al Haramain,* 686 F.3d at 987; *Zevallos* v. *Obama,* 10 F. Supp. 3d 111, 127 (D.D.C. 2014), *aff'd,* 793 F.3d 106 (D.C. Cir. 2015). The Department is committed to implementing the regulations consistent with constitutional requirements, and declines this commenter's suggestion to categorically limit designations to foreign persons.

One commenter requested that the Department affirmatively authorize academic researchers engaged in international research involving government-related data or bulk U.S. sensitive personal data to rely on documentation from international researchers outside a country of concern certifying that the international researchers are not covered persons. The Department declines to adopt this brightline rule. The Department expects U.S. persons engaged in data transactions involving access by countries of concern or covered persons to government-related data or bulk U.S. sensitive personal data to develop reasonable due diligence processes to ensure that they are not knowingly engaging in a covered data transaction with a covered person or country of concern. Notably, the prohibitions and restrictions in subparts C and D only apply to covered data transactions in which U.S. persons knowingly engage with countries of concern or covered persons. The reasonableness of those due diligence requirements will vary depending on the nature of the U.S. person engaging in such transactions; the counterparties with whom the U.S. person is engaging; and the volume, purpose, and nature of the bulk U.S. sensitive personal data or government-related data involved in the data transaction. For example, under some circumstances, it may be reasonable for a U.S. person to rely on certifications with supporting documentation from a foreign person that the foreign person is not a covered person. However, in light of the varying circumstances identified above, the Department declines to adopt a brightline rule about what specific due diligence mechanisms would apply.

G. Subpart H—Licensing

The proposed rule provided processes for regulated parties to seek, and for the Department to issue, general and specific licenses. As described in the NPRM, general licenses would be published in the **Federal Register** and could be relied upon by all relevant parties affected by a particular element of the regulations.[194] The Department anticipates that licenses will be issued only in rare circumstances as the Department deems appropriate. 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

[192] 89 FR 86151.

[193] *Id.*

[194] 89 FR 86151–52.

authorize only the transactions described in the license; a specific license might authorize one or more transactions that would otherwise be prohibited.

One commenter noted that the proposed rule did not provide clarity regarding how companies can seek requests for general licenses, nor a timeline for the Department to respond to a request for a general license. The commenter recommended that general licenses mimic OFAC's general licenses for medicines, which list a broad range of permitted activities. They also suggested that the Department include a mechanism for emergency authorization or expedited licenses to cover multiple data transfers, so that companies do not have to seek a license for each data transfer.

Companies seeking licenses should submit requests for specific licenses, not general licenses. The Department will determine and issue, at its discretion, general licenses in particular circumstances, such as where multiple companies in the same industry submit requests for specific licenses on the same topic, or in circumstances where the Department otherwise learns of a need to issue a general license, such as via industry engagement. The Department intends for general licenses to reflect some of OFAC's practices, and the Department has and will continue to examine those licenses to identify ways to structure the Department's general licenses. The Department anticipates that licenses—whether specific or general—will, in some cases, cover multiple data transactions in the same area, and that companies will not have to seek licenses for each data transfer. The Department also intends to consider emergency requests for specific licenses and, potentially, to issue general licenses that respond to emergencies, depending on the circumstances.

One commenter asked for clarification regarding how companies should submit requests for specific licenses. Section 202.802 describes that process, and the Paperwork Reduction Act submission that accompanied the proposed rule identified the information that an applicant would need to provide to the Department as part of a specific license application.[195] The Department intends to issue additional guidance to further describe the process for submitting specific license requests to help guide the regulated community.

One commenter expressed concern that, given that the Department has stated that licensing decisions will rarely be granted and will presumptively be denied, relying on licensing could raise the risk and cost of doing business in the biopharmaceutical sector, and will have scientific and business consequences for U.S. biotechnology companies. The Department recognizes the importance of promoting scientific research and biopharmaceutical developments to the U.S. economy, as well as to global health and well-being. As described in part IV.D of this preamble, the rule includes important exemptions to mitigate the consequences and costs of the rule's prohibitions and restrictions on scientific and medical research, and to preserve the development of innovative treatments for diseases and other medical conditions. *See also* §§ 202.504, 202.507, 202.510, and 202.511. The Department has also sought to clarify, in part IV.D of this preamble and in examples associated with the exemptions in subpart E, how the rule will apply to certain data transactions related to scientific research and the development of new medical treatments to provide regulated entities greater certainty about the rule's effect on their activities and to reduce the costs of complying with the rule. Notwithstanding these exemptions and clarifications, the licensing regime set forth in subpart H provides an important mechanism for the Department to grant additional categorical and case-by-case exemptions to the rule to ensure that the Department effectively balances the pressing national security risks of country of concern access to government-related data and bulk U.S. sensitive personal data with the Department's interest in promoting U.S. leadership in scientific research and pharmaceutical and biotechnological development. The Department intends to issue additional public guidance about how regulated entities may apply licenses before the rule's effective date to aid such entities in applying for licenses

One commenter expressed concern about the Department's ability to oversee the large and consequential task of issuing licenses, and they encouraged the Department to seek additional input from industry groups that have expansive experience with other similar licensing processes. The commenter also suggested testing any licensing scheme before it goes live. The Department appreciates this comment and will take it into consideration and follow-up as useful with relevant stakeholders after issuance of the final rule.

One commenter urged the Department to firmly commit to responding to licensing requests on a timely basis, and asked that the Department automatically approve any licenses it does not respond to in 45 days. The commenter also asked that the Department clarify whether the 45-day period set forth in § 202.802 for the Department to endeavor to respond to a request for a specific license means that the Department may issue or deny a license 45 days from submission of a request, or that the Department may, for example, only issue an initial response seeking more information about a license by the end of the 45-day period.

The Department is committed to timely responding to requests for licenses. The Department will endeavor to respond to license requests swiftly to ensure that it has received all information relevant to a license, and to issue licensing decisions 45 days from when the Department has received all information from the parties necessary to make a licensing decision. However, the Department declines to automatically approve licenses that it has not responded to within 45 days, because, as discussed in part IV.G of this preamble, the issuance of licenses is an exception to the rule to allow for transactions that warrant licenses, not a default. Moreover, depending on the subject matter in the license request, the Department may need to seek input from other agencies with relevant expertise and must ensure that it has sufficient time to do so.

One commenter asserted that the NPRM's proposal to include additional obligations on companies as conditions of specific licenses could lead to uncertainty and confusion by adding case-by-case requirements. Although the Department appreciates this concern, the Department maintains that it is important to retain the flexibility to impose requirements on specific licenses so that it can adequately respond to the fact-specific transactions presented in each specific license request, while also determining how to protect, to the greatest extent possible, the sensitive personal data involved in the underlying transactions.

One commenter suggested requiring license applicants to demonstrate compliance with existing data security frameworks. The Department agrees that demonstrating adequate attention to data security is likely to be an important factor in licensing decisions, but it declines to require any particular substantive requirement with respect to specific licenses in order to preserve the flexibility that the license is meant to provide.

[195] 89 FR 86203.

H. Subpart I—Advisory Opinions

1. Section 202.901—Inquiries Concerning Application of This Part

The NPRM proposed a system whereby the Attorney General could provide guidance on the rule in the form of official guidance or written advisory opinions. The final rule adopts the NPRM's proposal. 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.

One commenter expressed appreciation that trade associations may seek guidance on behalf of their members. Another commenter asked whether the Department would issue standardized guidelines beyond advisory opinions once the rule has been published. In addition to publishing advisory opinions, the Department intends to 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.

One commenter also asked whether the responsibility for seeking advisory opinions lies with U.S. companies handling a transaction, or with foreign companies conducting business with U.S. companies. The decision to seek an advisory opinion from the Department about a specific, non-hypothetical transaction is entirely voluntary, and only U.S. persons who are parties to a transaction that the rule potential regulates, or an agent of that U.S. person-party, may seek an advisory opinion from the Department. Also, in implementing this rule, the Department is committed to continuing its robust engagement and outreach with stakeholders and foreign partners, which may identify broader issues appropriate for clarification in public guidance.

I. 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,[196] and it expressly directs the Department's rule to ''address the need for, as appropriate, recordkeeping and reporting of transactions to inform investigative, enforcement, and regulatory efforts.'' [197] As the Department stated in the NPRM, it is critical to maximize widespread compliance with the 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.

1. Section 202.1001—Due Diligence for Restricted Transactions

The NPRM proposed imposing affirmative due diligence requirements as a condition of engaging in a restricted transaction. The NPRM also proposed 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 transactions, 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 NPRM proposed affirmative recordkeeping requirements as a condition of engaging in a restricted transaction, and it required U.S. persons subject to these affirmative requirements to maintain documentation of their due diligence, in order 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.

One commenter raised an unsubstantiated concern about the recordkeeping and due diligence requirements associated with restricted transactions, making a blanket assertion that the application of such requirements would be inconceivable for restricted transactions. As a solution to this unsubstantiated concern, the commenter requested that the Department replace the proposed requirements with an information-sharing framework like the ones utilized by customs authorities with respect to supply-chain risk. Specifically, this commenter suggested that the Department replicate the approach taken by the Customs-Trade Partnership Against Terrorism, which the commenter described as a public-private partnership pioneered by DHS to protect the U.S. supply chain in the aftermath of the terrorist attacks of September 11, 2001. Under this partnership, the commenter noted, U.S. companies voluntarily invested in improving their digital and other supply chain security processes, and agreed to share information with the United States Government, in exchange for a series of regulatory incentives. The Department declines to make this change for several reasons.

First, the Department lacks discretion under the Order to convert the rule to a voluntary public-private partnership or information-sharing program. The Order directs the Department to issue a rule prohibiting and restricting classes of transactions that pose an unacceptable risk of enabling countries of concern or covered persons to access government-related data or bulk U.S. sensitive personal data, and that meet certain other criteria.

Second, a voluntary information-sharing partnership would not address the unacceptable risks to national security and foreign policy at the heart of the Order. As explained in the NPRM and part IV of this preamble, these risks are externalities that derive in large part from U.S. persons' choices to share government-related data and bulk U.S. sensitive personal data with countries of concern and covered persons that they can leverage to exploit that data. Like other national security risks and threats, the data security risks addressed by the Order and this rule result from the failure of the private market to adequately internalize and account for these collective national security and foreign policy costs. Unlike this rule, a voluntary information-sharing program would not correct that externality because such a program would allow U.S. persons to continue to choose to engage in covered data transactions that pose these unacceptable risks.

The same is true of the specific recordkeeping and other due diligence requirements for restricted transactions. Recordkeeping, security, and due diligence requirements were contemplated as key mitigative components of restricted transactions in both the ANPRM and NPRM, providing the public with ample opportunity to raise substantiated concerns. The recordkeeping, security, and due diligence requirements are designed 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 requirements are specifically tailored to those risks. The commenter does not describe how—even if their concern were substantiated—replacing the recordkeeping and other due diligence requirements with a voluntary information-sharing program would mitigate such national security and

[196] 89 FR 15423.

[197] 89 FR 15424.

foreign policy threats. The commenter also does not explain how a voluntary information-sharing program would adequately enable the Department to monitor compliance with the rule, investigate potential violations, and enforce the rule, or ensure that U.S. persons are taking adequate steps to closely monitor their compliance with the rule given the risks posed by ongoing restricted transactions. The Department believes that these requirements are a critical part of mitigating the unacceptable risks posed by these transactions.

Third, the rule creates mechanisms for the Department to provide official guidance or written advisory opinions in response to specific inquiries received through advisory opinion procedures. As part of this system, the Department also 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 system will assist regulated parties in their application of the regulation's recordkeeping and due diligence requirements to specific, non-hypothetical factual scenarios.

Another commenter generally claimed that the final rule will impose significant compliance burdens on U.S. companies. The due diligence requirements for engaging in restricted transactions and the recordkeeping requirements that apply to both prohibited and restricted transactions are based on existing compliance expectations set by other regulators, such as OFAC and BIS, for screening vendors and transaction counterparties.

Another commenter claimed that costs to businesses for Know Your Customer (''KYC'') due diligence are generally already high, and that unclear requirements will add to business costs and frustration. The commenter stated that some information, such as an entity's residence or country of incorporation, may be easy to obtain, but the extent to which an entity is subject to the influence or control of a country of concern or covered person may not be readily apparent. Again, the Department cannot address this commenter's concerns because the commenter did not provide any specific information or justification for why the proposed rule's KYC requirements are unclear. However, as explained in the NPRM, the proposed rule does not require U.S. persons to determine whether an entity is controlled or subject to the influence of a country of concern. Regulated parties have the duty to determine whether entities or individuals meet the definitions of covered persons set forth in § 202.211(a)(1) through (4), none of which include control or influence. Rather, the Department will determine whether an entity is subject to the direction or control of a country of concern or covered person and, if so, will publicly designate them as a covered person. For this fifth category of covered persons, U.S. businesses need only rely on the published Covered Persons List when conducting due diligence.

Another commenter asserted that the proposed rule's due diligence, reporting and auditing requirements would impose a substantial administrative burden, and they recommended that the Department view due diligence requirements in proportion to the degree of risk associated with a covered data transaction. For example, the commenter suggested that due diligence for ''lower-risk'' transactions could include streamlined measures such as contractual safeguards and automated review of counterparties' technical indicators, such as IP address locations. As the Department discussed in the NPRM, the Department will encourage U.S. persons subject to the proposed rule to develop, implement, and update compliance programs as appropriate.[198] Although the Department may issue guidance to assist U.S. persons to develop and implement compliance programs, 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. Depending on a U.S. person's individualized risk profile, a reasonable compliance program could include streamlined measures such as contractual safeguards and automated review of counterparties' technical indicators, such as IP address locations.

Another commenter stated that multinational companies already have robust data privacy and export control programs that may be leveraged to comply with the rule, arguing that companies should not be required to set up entirely new compliance programs and should leverage existing compliance infrastructure to the extent feasible. Another commenter echoed the view that companies should be able to leverage existing privacy and data security programs. The Department strongly agrees. Nothing in the rule requires companies to set up new compliance programs where they already have such programs that otherwise meet the requirements of the rule. The Department expects that many companies will adapt their existing compliance programs to respond to the rule's requirements.

One commenter asserted, without support, that the proposed rule's due diligence requirements are akin to requiring that Post Offices read the mail of U.S. citizens and produce reports to law enforcement on what they have read. The commenter questioned whether the proposed rule conforms with the U.S. Constitution, described the due diligence and reporting requirements as a ''surveillance mandate,'' asserted that the rule contains serious civil rights concerns, and flagged that the NPRM docket did not reflect input from entities like the Department of State's Bureau of Democracy and Human Rights, the American Civil Liberties Union, or Freedom House.

This comment distorted and mischaracterized the rule in conclusory ways without any specificity or analysis of the rule itself. First, as explained in part L of this preamble, the ANPRM, NPRM, and this rule each resulted from extensive, robust formal and informal interagency review and input from dozens of agencies (including the State Department), White House offices, and other Executive Branch entities.

Second, the rule exempts from its coverage expressive information or informational materials and personal communications, among other things, and is consistent with the First Amendment, as discussed in part IV.D.1 of this preamble.

Third, the rule's due diligence and reporting requirements are tailored to ensure compliance and help inform the Department's administration of the program. The rule affirmatively requires due diligence and annual audits only for U.S. persons engaging in restricted transactions, and the due diligence requirements are similar to the elements of companies' compliance programs in the sanctions compliance and export controls contexts (although, in contrast to sanctions, which impose strict liability for violations, the rule's prohibitions include a knowledge standard). *See* § 202.1002. The rule requires reports only for a certain subset of restricted transactions that raise heightened risks, or where U.S. entities receive and reject offers to engage in a prohibited transaction involving data brokerage to help inform the Department about entities engaging in data brokerage that may be seeking to

[198] 89 FR 86152–53.

undermine or violate the rules. *See* § 202.1104. And much of the rule's recordkeeping requirements are in line with documents that businesses already keep, such as access logs.

Other than breezily using the buzzwords ''surveillance mandate'' to mischaracterize the rule's compliance requirements, the commenter did not describe what civil rights or constitutional concerns the proposed rule raises. The American Civil Liberties Union provided a comment to the proposed rule and did not raise the concerns asserted by the commenter. And although all members of the public had the opportunity to comment on the ANPRM and NPRM, Freedom House did not submit a comment. The commenter's buzzwords and unsupported accusations have no basis in the rule itself and provide no reason to alter the rule.

2. Section 202.1002—Audits for Restricted Transactions

The NPRM proposed imposing an annual audit requirement as a condition of engaging in a restricted transaction to verify and improve compliance with the security requirements. Section 202.1002(f) of the NPRM proposed requiring an auditor to submit a written report that describes the audit methodology, including ''the policies and other documents reviewed, personnel interviewed, and any facilities, equipment, networks, or systems examined.'' [199]

One commenter requested that the Department change this provision to insert the terms ''relevant'' before the terms ''policies,'' ''personnel,'' and ''facilities'' to ensure that auditors do not randomly review all the documents, personnel, or equipment of relevant parties. This comment appears to misinterpret the audit section of the proposed rule by reading § 202.1002(f) in isolation from § 202.1002's other provisions. Section 202.1002(e) of the proposed rule defined the scope of the audit and was already limited to focus only on activities covered by the proposed rule. In contrast, § 202.1002(f) addressed only what an auditor must include in the audit report.[200] It does not require an auditor to review all of a companies' policies, interview all its personnel, or examine all its facilities, equipment, networks or systems. However, to ensure that the regulatory text is clear, the final rule adds the term ''relevant'' to § 202.1002(f)(2)(ii) to clarify that the audit report must describe only the relevant policies, personnel interviewed, and facilities, equipment, networks or systems examined by the auditor.

A couple of commenters expressed concerns that the proposed rule did not include protections for confidentiality and trade secrets contained in reports and audits from either public disclosure or evidentiary use. It is unclear why the commenter thinks that the Department would not use an audit report as evidentiary support for an enforcement action if the report demonstrates a company's failure to comply with the rule. The audit report is one of the ways that the Department seeks to impose broad compliance with the rule. As for confidentiality, the Department would be bound by existing legal requirements regarding the protection of confidential or proprietary information.[201]

A number of commenters requested that companies be allowed to use audits completed for other purposes to comply with the final rule to avoid imposing significant compliance burdens on companies. The Department agrees with these comments and notes that the proposed rule required that a company conduct an audit of its compliance with the proposed rule, but it did not require that a company conduct a separate audit to comply with the audit requirements. The final rule does not include that requirement, either. However, the audit must specifically, sufficiently, and expressly address the requirements set forth in the rule.

Multiple commenters requested that companies be allowed to use internal auditors to audit compliance with the rule and reduce their compliance burden for restricted transaction. In the Department's extensive experience with corporate compliance in national security, criminal, and other contexts, internal audits often lack the independence, expertise, and resources to conduct objective and thorough evaluations of their own company's compliance efforts, while external audits often provide more effective and comprehensive assessments. However, the Department recognizes that, with the appropriate independence, expertise, and resources, internal audits may also be effective and may be a sensible part of a compliance program, depending on the U.S. company's individualized risk profile. The Department has thus updated the rule to delete the requirement that audits be ''external'' to allow internal audits that are otherwise sufficiently ''independent.'' The Department intends to provide additional guidance on the requirements for a sufficiently independent audit after the final rule is published.

One commenter suggested that the Department adopt a self-certification system akin to the Data Privacy Framework, and that the Department allow for third-party reviews as a condition for engaging in restricted transactions. Although the Department appreciates the value of certifications to privacy regimes such as the Data Privacy Framework, it does not find self-certifications sufficient to ensure compliance given the national security risks to government-related data and bulk U.S. sensitive personal data that the rule seeks to address. The audit provisions set forth in § 202.1002 are tailored to ensure compliance with the rule, including the security requirements, and to ensure that auditors have the requisite independence to effectively assess compliance.

One commenter claimed that the audit requirement in the proposed rule is unnecessarily broad because it would apply to all data transactions, straying beyond the national security concerns behind the proposed rule and imposing challenging requirements on U.S. companies. The commenter suggested that the Department consider a risk-based approach to auditing that takes into account the sensitivity of the data and the nature of transactions and counterparties, rather than imposing a uniform, annual auditing cadence for all restricted transactions. A few commenters also stated that an annual auditing requirement was burdensome. One commenter suggested that companies be allowed to conduct random spot audits, or that the Department require audits for companies engaged in high volumes of restricted transactions. Another commenter suggested that companies only be required to conduct audits after determining that they are not in compliance with the rule.

The audit requirement in the proposed rule explicitly applies only to U.S. persons engaging in restricted transactions; it does not apply broadly to all U.S. persons engaging in data transactions. No change is necessary to clarify this point. However, the Department appreciates that the scope of the audit provision in the NPRM's proposed § 202.1002(e)(1) could be read to apply to all data transactions, even those outside the scope of the rule, and has revised the terminology in § 202.1002(e)(1) in the final rule to clarify that the scope of the audit must examine a U.S. person's restricted transactions, not all their data transactions, and has revised

[199] 89 FR 86224.

[200] *Id.*

[201] *See, e.g.,* 28 CFR 16.7.

§ 202.1002(f)(2) to clarify that the audit report need only address the nature of a U.S. person's restricted transactions. The Department expects that an auditor would need to review a U.S. entity's procedures for determining whether transactions are restricted, prohibited, or exempt to ensure that the entity is appropriately identifying and handling restricted transactions. Once the auditing requirement is triggered, the rule would require the auditor to examine the data transactions engaged in by a U.S. person that it has identified as restricted transactions and determine whether the data transactions satisfy the CISA security requirements and other compliance obligations.

The proposed rule already took into account the sensitivity and nature of the transactions and counterparties by limiting the scope of the proposed rule's restrictions to countries of concern or covered persons, and by including bulk thresholds that trigger the rule's requirements. The Department believes that annual audits are necessary for U.S. persons to stay current with their data transactions and the security measures put in place to protect that data. Spot audits would provide only a snapshot in time and would not provide a company guidance about adequate remedial measures that they must take to come into compliance with the rule. Although one commenter noted that agencies monitoring CFIUS mitigation agreements often do not require annual audits, the commenter does not appear to consider that CFIUS mitigation agreements may contain other reporting obligations that can apprise CFIUS monitoring agencies, on a potentially regular basis, about a company's compliance with CFIUS mitigation without the need for an annual audit. The rule does not contain comparable reporting obligations. Furthermore, without auditing, it is unclear how a U.S. entity would adequately determine whether it is in compliance with the rule. For these reasons, the Department makes no changes on this issue.

J. Subpart K—Reporting and Recordkeeping Requirements

1. Section 202.1101—Records and Recordkeeping Requirements

The NPRM proposed requiring any U.S. person engaging in a restricted transaction to keep full and accurate records of each restricted transaction and to keep these records available for examination for at least 10 years after the date of each transaction (the length of the statute of limitations for violations of IEEPA). The proposed rule described 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.

One commenter repeated their claim from the ANPRM that this provision amounts to real-time, U.S. law enforcement-directed monitoring of data transmissions of private citizens and companies. This comment has no basis in the rule. As the NPRM explained, nothing in the rule, on its face or in practice, requires U.S. companies to surveil their employees, customers, or other private entities. All that § 202.1101 does is require U.S. persons that engage in restricted transactions to have and implement a risk-based compliance program, a common feature in sanctions, export controls, anti-money laundering, privacy, and a host of national security and other laws.

The EU's GDPR, for example, requires every data controller to ''maintain a record of the processing activities under its responsibility,'' including ''the purposes of the processing,'' ''a description of the categories of data subjects and of the categories of personal data,'' ''the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations,'' ''where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards,'' ''where possible, the envisaged time limits for erasure of the different categories of data,'' and ''where possible, a general description of the technical and organisational security measures referred to in Article 32(1).'' [202] The GDPR also requires data processors to similarly ''maintain a record of all categories of processing activities carried out on behalf of a controller.'' [203] And the GDPR requires data controllers and processors to make these records available to the relevant government authorities on request.[204] Similarly, the California Privacy Rights Act requires the issuance of regulations ''requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security'' to, among other things, ''perform a cybersecurity audit on an annual basis, including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent,'' and ''submit to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal information.'' [205] Other State privacy laws require similar audits, data protection assessments, and reporting.[206]

It is unclear why the commenter believes that similarly requiring U.S. persons to monitor their own transactions and their own compliance with this rule, and to use an audit to double-check their compliance and identify areas of non-compliance, equates to a surreptitious law-enforcement surveillance dragnet. The rule has nothing do to with the United States Government's authorities to lawfully engage in law enforcement and national security activities to gather intelligence. Personal communications, expressive information, and metadata ordinarily associated with expressive materials (or that is reasonably necessary to enable the transmission or dissemination of expressive materials) are specifically excluded from the scope of the rule. And the rule does not regulate purely domestic transactions between U.S. persons, like the collection, maintenance, processing, or use of data by U.S. persons within the United States (unless one of those persons is a publicly designated covered person).

Nor do the recordkeeping, reporting, or other requirements of the rule amount to a mechanism for the Federal Government to obtain access to the underlying data of U.S. persons. Nothing in the rule requires regulated parties to submit the underlying sensitive personal data to the Federal Government. For example, the annual reporting requirement in § 202.1103 for certain restricted transactions and the requirement in § 202.1104 to report certain rejected transactions require only a top-level description of the covered data transaction, such as the ''types and volumes'' of data involved in the transaction and the ''method of data transfer.'' The Department expects that

[202] Regulation (EU) 2016/679, *supra* note 153, art. 30(1).

[203] *Id.,* art. 30(2).

[204] *Id.,* art. 30(4).

[205] Cal. Civ. Code sec. 1798.185(a)(15).

[206] *See, e.g.,* Colo. Rev. Stat. 6–1–1302(c), 6–1–1309; 4 Colo. Code Reg. 904–3, Part 8; Conn. Gen. Stat. 42–522.

U.S. persons will fulfill these requirements by including only generalized statements in the report, such as ''15,000 U.S. persons' human genomic data transferred by file transfer protocol,'' without providing any of the underlying data.

To be sure, there may be limited circumstances in which the Department may need greater details about the underlying sensitive personal data, such as if a company seeks an advisory opinion about whether a certain kind of data meets one of the definitions for a category of sensitive personal data, or if a U.S. person applies for a specific license and adjudicating that license requires more details about the kinds of data that are the subject of the transaction, or if a company's non-compliance with the rule and any enforcement action turns on a dispute over the data itself. But in the Department's experience, even those limited circumstances should ordinarily be resolvable without needing access to the underlying data itself—such as through asking questions about the nature of the data to the parties, similar to what occurs in other national-security processes such as CFIUS and the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector.

Several commenters suggested that the Department include rules to protect companies' confidential information, proprietary information, or trade secrets to ensure that such information will not be publicly disclosed or used for evidentiary purposes. No change was made in response to this comment. These kinds of protections are already enshrined in other, longstanding laws (such as the Freedom of Information Act and Trade Secrets Act), and the rule will comply with them to the extent that they apply. Creating additional restrictions on the disclosure or use of such information is unnecessary and could undermine the Department's ability to investigate potential violations of the rule and enforce it.

Another commenter observed that many U.S. companies do not transact in data, but rather their data movement is part of a system or workflow. According to the commenter, the rule's recordkeeping requirements presume that companies have identified and isolated all discrete restricted transactions, but that is far more burdensome to do when data are part of globally integrated workflows. They described an example in which an engineer at a company responsible for product development or de-bugging may have routine access to user data and claim that those workflows make it more practical and cost-effective to more broadly adopt the requisite security requirements than to apply them in a piecemeal fashion. The Department appreciates that this rule will result in some compliance costs, but no change appears necessary to address this comment. The recordkeeping requirements do not presume that U.S. persons engage in only discretely identified restricted transactions. Indeed, the comment's suggested approach to its own example appears to be a workable solution based on the limited facts provided and, depending on the specific circumstances of a company, may be how some companies decide to reasonably comply with these regulations.

2. Section 202.1102—Reports To Be Furnished on Demand

The proposed rule included provisions to assist the Department in investigating potential noncompliance with the rule. These provisions 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.

One commenter stated that § 202.1102 is a means for U.S. companies to disclose and produce information upon demand to law enforcement authorities. No change was made in response to this comment. Section 202.1102 merely states the statutory recordkeeping and subpoena authority granted to the President and delegated to the Department under the Order. It is no different than other IEEPA recordkeeping and subpoena authority implemented by the Department of the Treasury across its sanctions programs or by the Department of Commerce under Executive Orders 13873 and 14034.

This same commenter also asserts that the requirements of § 202.1102 would impose significant budgetary expenses on the United States Government, which would be tasked with reviewing information on what the commenter asserted, without support, are billions of ''low-risk'' transmissions and millions of low-risk transactions. This comment merely repeated this commenter's claim that the restricted transactions are ''low risk,'' which has been addressed separately in part IV.C.1 of this preamble. The comment provided no specific analysis as to the number of non-exempt covered data transactions that are subject to the restrictions in this rule or the expenses that the commenter believes are required to implement the rule. And nothing in the rule establishes a program that requires the Department to review and approve data transmissions or transactions in advance. To the contrary, a hallmark of risk-based compliance is that the private sector, which is best positioned to know its own transactions, is responsible for managing its own compliance without the need for advance United States Government review and approval of every individual transaction undertaken, similar to approaches used for sanctions and export controls. While the rule does allow the Department to ask for records and institutes discrete reporting requirements for rejected transactions and for certain high-risk entities on an annual basis, it does not mandate that all such records be produced for the Department. The Department declines to make any changes to the rule based on this comment.

The same commenter expressed concern that the reporting provisions set out in subpart K could require some regulated entities, such as electronic communications services providers subject to the restrictions of 18 U.S.C. 2701 *et seq.,* to report information about transactions with their customers that Federal law may otherwise prohibit in the absence of specified legal process. The Department does not take a position regarding the commenter's legal analysis. However, the Department does not intend for regulated entities to construe the reporting provisions set forth in subpart K to impose reporting requirements inconsistent with Federal law. The Department has revised the provisions in subpart K to clarify that the reporting requirements do not oblige parties to furnish information in reports that Federal law would otherwise prohibit.

Another commenter in the pharmaceutical research field argued that their current auditing and recordkeeping measures already adhere to much of what is required under the NPRM, and asserted that it would be unduly burdensome for them to repeat these efforts. Nothing in the rule requires U.S. persons to unnecessarily duplicate their records or create redundant systems. U.S. persons can use existing auditing, recordkeeping, and other compliance practices and systems to the extent that they fully satisfy the requirements of this rule.

3. Section 202.1104—Reports on Rejected Prohibited Transactions

The NPRM proposed requiring 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.

One commenter noted that a 14-day period for reporting on rejected transactions should be extended to a minimum of 30 days. The commenter argued that 14 days was too narrow from a compliance standpoint and that 30 days would allow companies sufficient time to investigate, document, and confirm relevant details about a rejected transaction. The Department declines to adopt this suggested change. While the Department appreciates the desire for a longer reporting period, the proposed 14-day period is consistent with, and indeed longer than, the similar reporting period implemented by OFAC, which requires reporting on rejected transactions within 10 business days of rejecting such a transaction.[207] 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 rule, including through evasion. The information submitted by these reports will thus assist the Department in monitoring U.S. persons' compliance with the rule, identifying matters for potential investigation, undertaking enforcement actions, and identifying ways in which to refine the rule in the future. Additionally, timely reporting of a rejected transaction could, in real time, potentially curtail adversaries' future attempts to access government-related data or bulk U.S. sensitive personal data because the Department can promptly uncover conspiracies to evade or avoid the rule's prohibitions, identify shell companies and agents, investigate targets for designation or enforcement actions, and mitigate potentially ongoing threats to U.S. national security, which increase the longer a rejected restricted transaction goes unreported. Furthermore, lengthening the deadline is unnecessary to allow investigation and documentation because § 202.1104(c) already limits reports on rejected transactions to the required information ''to the extent known and available to the person filing the report at the time the transaction is rejected.'' The Department thus expects that U.S. persons will generally satisfy this reporting requirement by filing an initial report with the information known at the time the transaction is rejected and supplementing it later with additional documentation or relevant details from the results of their investigations, or as requested by the Department. The Department thus declines to change the timeframe.

K. Subpart M—Penalties and Finding of Violation

The NPRM proposed civil and criminal penalties, including a process for imposing civil monetary penalties similar to those used in other IEEPA-based regimes.

One commenter requested reduced criminal penalties, noting that the penalties of up to 20 years in prison seem ''quite punitive'' for a covered data transaction violation. The Department declines to take an approach that would create an inconsistency with other penalties imposed for IEEPA-based criminal violations. Under IEEPA, criminal penalties apply to any person convicted of willfully committing, willfully attempting to commit, willfully conspiring to commit, or aiding or abetting in the commission of a violation of any license, order, regulation, or prohibition issued under IEEPA. The penalties, as stated in the NPRM, are commensurate with the willful actions of the person on whom the Department imposes such penalties. The Department further notes that these penalties are intentionally designed to be severe, reflecting the gravity of the national security risks associated with violating the rule and its provisions, and are intended to deter and prevent violations of the prohibitions. Finally, the provisions of IEEPA allow the Department to exercise its discretion. Upon conviction, criminal violators may be fined not more than $1,000,000, or if a natural person, may be imprisoned for not more than 20 years, or both. As with all Federal criminal cases, unless a criminal penalty has a mandatory minimum sentence (which the rule does not), the ultimate penalty, up to the statutory maximum, will be imposed by a Federal district judge, who will determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors.

Another commenter recommended that if an entity in compliance with the rule makes a voluntary self-disclosure (''VSD'') to the Department about a possible violation of the rule, that entity should receive ''safe harbor'' (presumably from any civil or criminal enforcement action, although the commenter did not specify) to encourage proactive participation in compliance mechanisms. In that vein, the Department intends to publish compliance and enforcement guidance and other resources to help the regulated community comply with the rule. Similar to guidance published by the Department regarding other VSD programs,[208] the Department anticipates that the guidance and resources regarding the rule will cover a variety of issues and will likely include a discussion of how the Department will assess VSD.

L. Coordination With Other Regulatory Regimes

The proposed rule discussed three potential areas of overlap between the proposed rule and existing regulatory regimes. First, the Department considered the potential interaction between this rule's application to investment agreements and CFIUS's authority to review ''covered transactions,'' *see generally* 50 U.S.C. 4565. Second, the Department considered, in consultation with the Federal Trade Commission (''FTC'') and other agencies, the potential interaction between this rule's application to data-brokerage transactions and PADFAA.[209] Third, the Department considered the potential interaction between this rule's application to vendor agreements and any actions taken by the Secretary of Commerce under Executive Orders 13873 and 14034.

One commenter recognized the Department's efforts to distinguish PADFAA from the proposed rule, but contended that the proposed rule is redundant in light of PADFAA, and urged the Department to incorporate provisions into the final rule to clarify which agency would take primary jurisdiction over activities that violate both PADFAA and this final rule. Another commenter urged the Department to coordinate with the FTC on enforcement activities because the FTC lacks experience addressing national security concerns and is not the appropriate agency to identify or determine whether an entity is controlled by a foreign adversary. Another commenter requested that the Department sign a memorandum of understanding with the FTC to ensure cooperation.

As the Department discussed in the NPRM, the Department does not believe that it would be appropriate to alter the proposed rule's scope in light of PADFAA for several reasons.[210] There

[207] 31 CFR 501.604(c).

[208] *See, e.g.,* U.S. Dep't of Just., *Voluntary Self Disclosure and Monitor Selection Policies* (Mar. 8, 2024), *https://www.justice.gov/corporate-crime/voluntary-self-disclosure-and-monitor-selection-policies* [*https://perma.cc/SQ5N-5ECP*]; U.S. Dep't of Just., *Criminal Division Pilot Program on Voluntary Self-Disclosures for Individuals* (Sept. 19, 2024), *https://www.justice.gov/criminal/criminal-division-pilot-program-voluntary-self-disclosures-individuals* [*https://perma.cc/B845-NM3C*].

[209] Public Law 118–50, *supra* note 20.

[210] 89 FR 86155.

are significant differences in scope between PADFAA and the proposed rule, which the Department set forth in some detail in the NPRM, and which the commenters do not address. Although the Department declines to set forth which agency would take primary jurisdiction over enforcement actions, as the Department explained in the NPRM, 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.[211] For example, the Department and the FTC intend to coordinate, as appropriate, on licensing decisions and on any potential enforcement actions under PADFAA with respect to activities that may be authorized, exempt, or licensed under the rule.

For related reasons, the Department rejects one commenter's suggestion that the Department abandon the rulemaking because the enactment of PADFAA makes the President's declaration of an emergency unnecessary. As a legal matter, the President's declaration of an emergency is unreviewable by a court, and it is not a decision the Department is authorized to revisit. And, substantively, the rule covers a range of transactions—such as restricted transactions—that present the national security threats recognized by the President's declaration and the Order and that are entirely outside PADFAA's scope. This suggestion also ignores the significant differences in scope and structure between the Order and PADFAA, which the NPRM discussed.

Another commenter renewed a suggestion originally raised as a comment to the ANPRM that the Department address additional potential overlap between the proposed rule and the ICTS program and its rules relevant to sensitive data, the BIS NPRM regarding the requirements for Infrastructure as a Service (''IaaS'') providers to verify the identity of foreign customers,[212] and the BIS ANPRM regarding connected vehicles.[213] The Department has already considered and discussed the potential interaction between this rule and actions that the Secretary of Commerce may take, as authorized by Executive Orders 13873 and 14034, and the commenter does not engage with the analysis provided in the Department's NPRM. Furthermore, the Department of Commerce has not yet issued final rules regulating IaaS or connected vehicles, so it would be premature to provide an analysis of the ways in which the Department's rule interacts with those rules. As noted in the NPRM, the Department is committed to working with BIS to ensure a consistent approach between the rule's restrictions on vendor agreements and any ICTS actions that may overlap.

One commenter argued that, on issues that depend on public and private information exchanges with U.S. allies and trading partners—such as commerce, diplomacy, health, science, and technology—the NPRM did not adequately address the damage that would be done to the long-established regulatory processes and policy interests of other agencies, including the Department of Commerce, Department of State, and HHS. The Department disagrees. The interagency process to develop the Order, ANPRM, and NPRM included review by and consultation with dozens of Federal departments and agencies, including those listed by the commenter. The Department consulted a broad range of agencies, White House offices, and other Executive Branch entities, including the Departments of State, Treasury, Defense, Commerce, HHS (including the FDA, NIH, and Centers for Disease Control and Prevention), Veterans Affairs, and DHS; the U.S. Postal Service; the U.S. Intelligence Community; White House offices such as the Office of Pandemic Preparedness, OMB (including the Office of Information and Regulatory Affairs (''OIRA'')), Office of the National Cyber Director, Domestic Policy Council, Council of Economic Advisors, and National Economic Council; the National Security Council (including the International Economics, Technology & National Security, Global Health Security & Biodefense, China, Cyber, and Legal directorates); the Office of the U.S. Trade Representative; the FTC; the Federal Communications Commission; the Consumer Financial Protection Bureau; the National Science Foundation; the SEC; the Board of Governors of the Federal Reserve; the Federal Deposit Insurance Corporation; and the Commodity Futures Trading Commission. The final rule is a reflection of the Department's extensive efforts at whole-of-government coordination. At each interval of the rulemaking process, departments and agencies have had the opportunity to provide, and have provided, meaningful and extensive input to the Order, ANPRM, NPRM, and final rule.

Another commenter expressed support for the Department's coordination with other regulatory regimes, noting that companies involved in international trade are already subject to national security-related requirements overseen by CFIUS, OFAC, BIS, and other entities. The commenter noted that efforts to harmonize the various applicable regimes will be greatly beneficial to the companies seeking to comply.

M. Severability

Section 202.106 of the NPRM provided that the provisions of this rule are intended to be severable from each other if any provision of the final rule 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 Department did not receive any comments on § 202.106 and adopts and slightly amends it, with the additional explanation below.

The Department has determined that this rule implements and is fully consistent with governing law, but it recognizes that implementation may be subject to legal challenge. The Department intends for the provisions of this rule to be severable from each other. The Supreme Court has explained that where specific provisions of a rule are unlawful, severance is preferred when doing so ''will not impair the function of the [rule] as a whole, and there is no indication that the regulation would not have been based but for its inclusion.'' [214]

In the event 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. Each provision of the final rule and application thereof serves an important, related, but distinct purpose; provides a distinct benefit separate from, and in addition to, the benefit provided by other provisions and applications; is supported by evidence and findings that stand independent of each other; and is

[211] *Id.*

[212] Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities, 89 FR 5698 (Jan. 29, 2024) (to be codified at 15 CFR pt. 7).

[213] 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).

[214] *K Mart Corp.* v. *Cartier, Inc.,* 486 U.S. 281, 294 (1988); *see also Sw. Elec. Power Co.* v. *EPA,* 920 F.3d 999, 1033 (5th Cir. 2019) (vacating only challenged portions of a rule).

capable of operating independently such that the invalidity of any particular provision or application would not undermine the operability or usefulness of other aspects of the final rule. Depending on the circumstances and the scope of a 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. Although more limited application may change the magnitude of the overall benefit of the final rule, it would not undermine the important benefit of, and justification for, the final rule's application to other persons or circumstances. The qualitative and quantitative benefits of the final rule outweigh the costs for all persons and circumstances covered by the final rule.

For example, the prohibitions and restrictions related to transactions involving access to personal health data should continue to apply even if a court holds that the restrictions or prohibitions on transactions involving access to biometric data are invalid. Similarly, the rest of the conditions required for U.S. persons to engage in restricted transactions with a country of concern or covered person should continue to apply even if a court holds that one set of conditions (such as the recordkeeping requirements) are invalid. The rule should also continue to apply with respect to other countries of concern (such as North Korea) or categories of covered persons even if a court finds its application with respect to one country of concern (such as Russia) or one category of covered persons is invalid. The Department's intent that sections and provisions of the final rule can function independently similarly applies to the other portions of the rule.

N. Other Comments

One commenter recommended that the Department consider amending the rule to require Federal agencies to implement universal opt-out mechanisms (''UOOMs'') on government devices at the operating system level and that the Department ''work with state enforcers to ensure website and application compliance.'' According to this commenter, such mechanisms would prevent applications from accessing specific data on government devices and send a signal requesting websites and apps not to sell or share user data with third parties. This commenter remarked that such an amendment would offer a proactive approach to data protection that complements the rule's restrictions on certain data transactions by preventing sensitive government data from entering vulnerable data ecosystems in the first place.

While the Department appreciates this commenter's recommendation, the Order and this rule do not regulate the United States Government's own activities, including the operation of its own devices, as made clear by section 8 of the Order. This limitation would preclude the Department from requiring a UOOM on United States Government devices at the operating system level, as the commenter suggested. However, the Department has shared this recommendation with CISA and others within the United States Government that are focused on securing sensitive personal data on the United States Government's own systems and devices.

One commenter ''agree[d] that there needs to be regulation, including to a greater extent, of U.S. data,'' but noted that ''the rule falls short of an effective law.'' Another commenter noted that in light of the glaring need for national data protection against threats from abroad and recent data breaches, this rule may not go far enough, but it at least serves to set the foundation for a ''much needed wall against continued foreign threats.'' While the Department appreciates the concept raised by these commenters, the Order only authorizes the Department to promulgate regulations that prohibit or otherwise restrict transactions that present an unacceptable risk to national security by affording countries of concern or covered persons with access to government-related data and bulk U.S. sensitive personal data. As the Department has publicly explained, this rule is one key part of a broader solution to make it more difficult for countries of concern to obtain Americans' sensitive personal data. While this rule is focused on one set of risk vectors (access through commercial activities), other risk vectors such as theft and computer intrusions must necessarily be addressed by other complementary national security, cybersecurity, and privacy measures.

V. Regulatory Requirements

The Department designated the proposed rule as ''significant'' under Executive Order 12866, as amended.[215] Upon review, OIRA agreed with this designation. The Department has likewise designated this final rule as ''significant'' under Executive Order 12866, as amended, and OIRA has similarly concurred with that designation. Accordingly, this rule includes a Final Regulatory Impact Analysis (''FRIA'') and a Final Regulatory Flexibility Analysis (''FRFA''), as required by Executive Order 12866, as amended, and the Regulatory Flexibility Act,[216] respectively. Part V.A of this preamble summarizes the FRIA. The full version of the FRIA is available on *regulations.gov* (Docket No. NSD–104).

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

Pursuant to the requirements of Executive Order 12866, as amended, at section 6(a)(3)(C), the Department has prepared an FRIA of the potential economic impacts of this rule and placed the FRIA on this rule's docket on *regulations.gov* (Docket No. NSD–104). The FRIA evaluates the potential economic impacts of this final rule on entities in the United States that are likely to be affected by the rule.

The Department requested comments on the Initial Regulatory Impact Analysis (''IRIA''), including the economic impact of the proposed rule. The Department received several comments directed to the IRIA. A summary of and response to those comments are contained in the full FRIA that is found on *regulations.gov.*

The Department estimates the discounted annualized cost of the regulation to be approximately $459 million annually. The extremely high potential net benefits (*i.e.,* expected benefits less estimated costs) justify moving forward with the rule. The approximately $459 million in estimated annual cost would significantly protect U.S. national security, including well over 100 million American individuals who are potential targets of adversaries exploiting government-related data and bulk U.S. sensitive personal data. While the benefits to national security are difficult to quantify, the Department expects them to be substantial, including preventing the use of data by countries of concern and covered persons to micro-target U.S. persons, to aggregate insights from large datasets to target United States Government and private-sector activities, and to enhance military capabilities that include facilitating the development of bioweapons. Meanwhile, the estimated annual cost of the regulation is very low relative to the relevant economic activity. For example, the approximately $459 million in estimated annual cost of the rule is only about one-third of 1

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

[216] 5 U.S.C. 601 *et seq.*

percent (0.3 percent) of the $176 billion in revenues generated in the U.S. Computing, Infrastructure, Data Processing Services, and Web Hosting Services industry sector. The Department therefore expects that the national security and foreign policy benefits, while qualitative, will far outweigh the estimated costs of the final rule.

Although, as the FRIA notes, the monetary value of the data sold to countries of concern appears to represent a relatively small percentage of the overall value of all such transactions from U.S. entities, the data that is sold—especially when it is government-related data or bulk U.S. sensitive personal data—presents significant risks to U.S. persons and to U.S. national security. As explained more fully in part II of this preamble, countries of concern seek to obtain government-related data and bulk U.S. sensitive personal data for malicious uses that undermine the national security and foreign policy of the United States.

Overall, the Department estimates that this rule may directly financially impact approximately 3,000 companies engaged in data brokerage and an additional 1,500 firms that currently engage in restricted transactions involving government-related data and bulk U.S. sensitive personal data with covered persons. This is a relatively small fraction of the overall number of U.S. firms engaged in transactions involving bulk data, as the rule only affects those specific types of commercial transactions identified in the rule that involve access to government-related data or bulk U.S. sensitive personal data by the six identified countries of concern, or by covered persons. These annual costs may include lost and forgone transactions, the cost of deploying the CISA security requirements for restricted transactions, and the direct costs of compliance. Many of the compliance costs that regulated entities will incur due to the rule are one-time costs, such as initial assessments and remediation efforts, that will be needed only once to come into initial compliance with the rule's requirements. Other costs, such as monitoring, compliance audits, reporting, and training, will occur annually.

As the FRIA explains, the Department cannot assess whether any secondary impacts or indirect costs of this rule are reasonably likely given the limitations of available information, the resulting uncertainty, and the qualifications surrounding the analysis. Such impacts and costs are still too speculative and hypothetical to be quantified in this analysis. Even assuming, however, that such impacts and costs were reasonably likely and could be reasonably estimated, the Department would still conclude that the high qualitative and quantitative benefits to national security and foreign policy of this rule would outweigh the estimated impacts and costs. Additionally, the rule includes 11 exemptions that allow notable categories of commercial transactions to continue unimpeded by the rule's prohibitions and restrictions, and that reduce the overall costs of the rule. *See* §§ 202.501 through 202.511. Sections 202.800 through 202.803 further provide a mechanism for entities to obtain licenses for otherwise restricted or prohibited transactions.

Finally, the FRIA identifies both the baseline for the Department's cost estimates of the potential impact of the rule, as well as the assumptions used to determine that potential impact. These assumptions include estimates of the number of potentially impacted parties, the costs of compliance, and the number of potentially affected transactions. These assumptions are necessary because, as a new regulatory program, there is little data publicly available about the markets impacted by this rule. The assumptions are also over-inclusive in terms of the impact estimates because they rely on North American Industry Classification System (''NAICS'') codes that include entities likely not impacted by the rule, as well as transactions that will be exempted from the rule's prohibitions and restrictions. Nonetheless, the assumptions provide a best estimate of both the estimated costs and expected benefits of the rule, given available economic information. The FRIA also includes updated dollar amounts for various estimated impacts, most notably for the estimated total annual costs of compliance for this rule as well as the 10-year annualized cost estimates. The new figures are lower, though not significantly, than those projected in the IRIA included in the NPRM. The changes do not reflect substantially new data or analyses, but rather provide greater accuracy to the tables by correcting for previous rounding errors and unifying the data.

B. Regulatory Flexibility Act

The Department promulgates this rule to address the growing threat posed by the efforts of foreign adversaries to access and exploit government-related data or bulk U.S. sensitive personal data, as articulated in the Order. In particular, the 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 this rule is articulated in part II of and throughout this preamble. Briefly, advances in computing technology, AI, and methods for processing large datasets allow countries of concern to more effectively leverage for malicious purposes government-related or bulk U.S. sensitive personal data they have purchased or collected. The capability currently exists to allow anyone, including countries of concern, who have access to government-related data or 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 Rule

Through the Order, the President used his authority under IEEPA and the NEA to declare national emergencies and regulate certain types of economic transactions to protect the country against foreign threats. The Order expands upon the national emergency previously declared by Executive Order 13873, as modified by Executive Order 14034. 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 ''deal with any unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States,'' including by investigating, blocking, prohibiting, and regulating transactions involving ''any property in which any foreign country or a national thereof has any interest by any person, or with respect to any property, subject to the

jurisdiction of the United States.'' [217] Existing IEEPA-based programs include those administered by OFAC, which enforces economic and trade sanctions, and the BIS Office of Information and Communications Technology and Services, 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 Rule Will Apply

The rule will 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 (''small entities''), will be impacted by the rule. Therefore, the Department estimates that this rule will 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,[218] 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 at 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.[219] The Department estimated the likely number of small entities affected by the rule using the Small Business Administration (''SBA'') small business size standards, which themselves are based on the NAICS codes. According to the SBA Office of Size Standards, a small business under NAICS code 518210 has an annual revenue under $40 million.[220]

Under the appropriate NAICS code, data brokers are considered a subset of the total firms; 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 rule impacts a substantial number of small entities.

TABLE V–1—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 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 costs as a percentage of annual revenue will vary company by company.

The Department is not aware of recent 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 rule that falls on small firms is complicated by the fact that several of the 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 will still face a higher cost burden, proportionally, from the rule than larger firms. Large entities will likely already have a greater portion of the fixed costs associated with the 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.

3. Description of the Projected Reporting, Recordkeeping, and Other Compliance Requirements of the Rule

The rule requires firms engaged in restricted transactions to adhere to certain standards for data security, due diligence, recordkeeping, and reporting. *See* § 202.1101. 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 data security policies, practices, and requirements and data-level requirements developed by DHS through CISA in coordination with the Department. *See* § 202.248. Those requirements, which CISA is releasing and announcing through a **Federal Register** notice issued concurrently with the final rule, overlap with several similar, widely used cybersecurity standards or frameworks. In addition, the security requirements developed by CISA 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. As stated in part IV.I.2 of this preamble, the Department intends to provide additional guidance on the requirements for a sufficiently independent audit after the final rule is published.

Additionally, to ensure that government-related data and bulk U.S. sensitive personal data are not accessible by countries of concern or covered persons, the rule requires firms to engage in due diligence before pursuing restricted transactions, such as by using KYC/Know-Your-Vendor programs to complete background checks on potential partners. Furthermore, as described in § 202.1002 the rule requires firms to keep records that contain extensive details of their restricted transactions as well as the details of the other parties involved. They are also required to undergo

[217] 50 U.S.C. 1701(a), 1702(a)(1)(B).

[218] 5 U.S.C. 601 *et seq.*

[219] *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*].

[220] *Id.*

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 Rule

As discussed in part IV.L of the preamble, while PADFAA seeks to address some of the same national security risks as the rule does, there are clear differences between PADFAA, the Order, and this 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 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, this 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.L 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 rule could also end up being subject to review and action by CFIUS. In 2018, 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.[221]

However, while CFIUS acts on a transaction-by-transaction basis, this final rule creates restrictions and prohibitions on covered data transactions that apply to categories of data transactions involving the six countries of concern. In a situation where a covered data transaction otherwise subject to the rule is later subject to a CFIUS review, such transaction would be exempted from the Department's review under the rule to the extent that CFIUS takes any of the actions identified in the rule. *See* §§ 202.207 and 202.508.

Furthermore, the categories of covered data transactions covered by the rule extend beyond the scope of CFIUS, including, for example, the categories addressing the provision of government-related data or bulk U.S. sensitive personal data through data brokerage, vendor agreements, and employment agreements. The 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.

A description of the alternatives considered, the need for, and objectives of, the rule is included in section I.I. of the FRIA accompanying this rule, and is not repeated here.

C. Executive Order 13132 (Federalism)

The rule does not have federalism implications warranting the application of Executive Order 13132. The 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.

D. Executive Order 13175 (Consultation and Coordination With Indian Tribal Governments)

The rule does 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 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 rule have been approved by OMB in accordance with the Paperwork Reduction Act of 1995, 44 U.S.C. 3507, under control number 1124–0007.

The 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. The Department did not receive any comments specifically on these collections of information or the estimated burden.

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 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 two 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 two 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 five 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 two 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.

[221] *See* Public Law 115–232, tit. XVII, secs. 1701–28, 132 Stat. 1636, 2173.

• *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 $22,500,000 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 OMB.

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 one 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 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 rule.

H. Congressional Review Act

Pursuant to Subtitle E of the Small Business Regulatory Enforcement Fairness Act of 1996 (also known as the Congressional Review Act), the Office of Information and Regulatory Affairs has determined that this rule meets the criteria set forth in 5 U.S.C. 804(2). As laid out in the FRIA, this rule is expected to result in an annual effect on the economy of $100 million or more. The Department will submit the final rule to Congress and the U.S. Government Accountability Office consistent with the Congressional Review Act's requirements no later than its effective date.

I. Administrative Pay-As-You-Go Act of 2023

The Department has determined that the Administrative Pay-As-You-Go Act of 2023 (Pub. L. 118–5, div. B, title III, 137 Stat. 31 (2023)) does not apply to this rule because it does not affect direct spending.

List of Subjects in 28 CFR Part 202

Incorporation by reference, 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 adds part 202 to 28 CFR chapter I 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. For purposes of determining whether a transaction is a covered data transaction, access is determined without regard for the application or effect of any security requirements.

§ 202.202 Attorney General.

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

§ 202.203 Assistant Attorney General.

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

§ 202.204 Biometric identifiers.

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

§ 202.205 Bulk.

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

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

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

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

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

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

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

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

§ 202.206 Bulk U.S. sensitive personal data.

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

§ 202.207 CFIUS action.

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

(a) Suspension of a proposed or pending transaction, as authorized under 50 U.S.C. 4565(l)(1);

(b) Entry into or imposition of any agreement or condition with any party to a covered transaction, as authorized under 50 U.S.C. 4565(l)(3); and

(c) The establishment of interim protections for covered transactions withdrawn before CFIUS's review or investigation is completed, as authorized under 50 U.S.C. 4565(l)(5).

§ 202.208 China.

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

§ 202.209 Country of concern.

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

(a) Has engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons; and

(b) Poses a significant risk of exploiting government-related data or bulk U.S. sensitive personal data to the detriment of the national security of the United States or security and safety of U.S. persons.

§ 202.210 Covered data transaction.

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

(1) Data brokerage;

(2) A vendor agreement;

(3) An employment agreement; or

(4) An investment agreement.

(b) *Examples*—(1) *Example 1.* A U.S. institution conducts medical research at its own laboratory in a country of concern, including sending several U.S.-citizen employees to that laboratory to perform and assist with the research. The U.S. institution does not engage in data brokerage or a vendor, employment, or investment agreement that gives a covered person or country of concern access to government-related data or bulk U.S. sensitive personal data. Because the U.S. institution does not engage in any data brokerage or enter into a vendor, employment, or investment agreement, the U.S. institution's research activity is not a covered data transaction.

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

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

§ 202.211 Covered person.

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

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

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

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

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

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

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

§ 202.212 Covered personal identifiers.

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

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

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

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

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

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

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

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

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

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

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

(d) *Examples of a listed identifier in combination with other data disclosed by a transacting party*—(1) *Example 1.* A foreign person who is a covered person asks a U.S. company for a list of Media Access Control (''MAC'')

addresses from devices that have connected to the wireless network of a U.S. fast-food restaurant located in a particular government building. The U.S. company then sells the list of MAC addresses, without any other listed identifiers or sensitive personal data, to the covered person. The disclosed MAC addresses, when paired with the other data disclosed by the covered person—that the devices ''have connected to the wireless network of a U.S. fast-food restaurant located in a particular government building''—makes it so that the MAC addresses are linked or linkable to other sensitive personal data, in this case precise geolocation data of the location of the fast-food restaurant that the national security-related individuals frequent with their devices. This combination of data therefore meets the definition of covered personal identifiers.

(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, excluding an employment agreement, investment agreement, or a vendor agreement, involving the transfer of data from any person (the provider) to any other person (the recipient), where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data.

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

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

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

(4) *Example 4.* A U.S. company owns and operates a mobile app for U.S. users with available advertising space. As part of selling the advertising space, the U.S. company provides IP addresses and advertising IDs of more than 100,000 U.S. users' devices to an advertising exchange based in a country of concern in a twelve-month period. The U.S. company's provision of this data as part of the sale of advertising space is a covered data transaction involving data brokerage and is a prohibited transaction because IP addresses and advertising IDs are listed identifiers that satisfy the definition of bulk covered personal identifiers in this transaction.

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

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

(7) *Example 7.* A U.S. company owns or operates a mobile app or website for U.S. users. That mobile app or website contains one or more tracking pixels or software development kits that were knowingly installed or approved for incorporation into the app or website by the U.S. company. The tracking pixels or software development kits transfer or otherwise provide access to

government-related data or bulk U.S. sensitive personal data to a country of concern or covered person-owned social media app for targeted advertising. The U.S. company engages in prohibited data brokerage.

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

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

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

§ 202.215 Directing.

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

§ 202.216 Effective date.

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

§ 202.217 Employment agreement.

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

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

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

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

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

(5) *Example 5.* A U.S. company sells goods and collects bulk personal financial data about its U.S. customers. The U.S. company appoints a citizen of a country of concern, who is located in a country of concern, to its board of directors. This director would be a covered person, and the arrangement appointing the director would be an employment agreement. In connection with the board's data security and cybersecurity responsibilities, the director could access the bulk personal financial data. The director's employment would be a restricted transaction.

§ 202.218 Entity.

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

§ 202.219 Exempt transaction.

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

§ 202.220 Former senior official.

The term *former senior official* means either a ''former senior employee'' or a

''former very senior employee,'' as those terms are defined in 5 CFR 2641.104.

§ 202.221 Foreign person.

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

§ 202.222 Government-related data.

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

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

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

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

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

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

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

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

§ 202.223 Human biospecimens.

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

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

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

(3) 3001.90.0115 Glands and other organs, dried, whether or not powdered

(4) 3002.12.0010 Human blood plasma

(5) 3002.12.0020 Normal human blood sera, whether or not freeze-dried

(6) 3002.12.0030 Human immune blood sera

(7) 3002.12.0090 Antisera and other blood fractions, Other

(8) 3002.51.0000 Cell therapy products

(9) 3002.59.0000 Cell cultures, whether or not modified, Other

(10) 3002.90.5210 Whole human blood

(11) 3002.90.5250 Blood, human/animal, other

(12) 9705.21.0000 Human specimens and parts thereof

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

§ 202.224 Human 'omic data.

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

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

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

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

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

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

§ 202.225 IEEPA.

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

§ 202.226 Information or informational materials.

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

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

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

(2) Items that were, as of April 30, 1994, or that thereafter become, controlled for export to the extent that such controls promote the 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 U.S. sensitive personal data. The U.S. company offers, for a fee, to use data analytics to link the data across these databases to the same individuals and to sell that combined dataset to a covered person. This service constitutes a substantive alteration or enhancement of the data in the pre-existing databases and therefore is not information or informational materials.

§ 202.227 Interest.

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

§ 202.228 Investment agreement.

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

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

(2) A U.S. legal entity.

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

(1) Is made:

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

(ii) Into a security offered by:

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

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

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

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

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

(c) *Examples*—(1) *Example 1.* A U.S. company intends to build a data center located in a U.S. territory. The data center will store bulk personal health data on U.S. persons. A foreign private equity fund located in a country of concern agrees to provide capital for the construction of the data center in exchange for acquiring a majority ownership stake in the data center. The agreement that gives the private equity fund a stake in the data center is an investment agreement. The investment agreement is a restricted transaction.

(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 indicates, reveals, or describes 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 E.O. 14117 Implementation, January 2025. This material is incorporated by reference into this section with the approval of the Director of the Federal Register under 5 U.S.C. 552(a) and 1 CFR part 51. This incorporation by reference (''IBR'') material is available for inspection at the Department of Justice and at the

National Archives and Records Administration (''NARA''). Please contact the Foreign Investment Review Section, National Security Division, U.S. Department of Justice, 175 N St. NE, Washington, DC 20002, telephone: 202–514–8648, *NSD.FIRS.datasecurity@usdoj.gov; www.justice.gov/nsd.* For information on the availability of this material at NARA, visit *www.archives.gov/federal-register/cfr/ibr-locations* or email *fr.inspection@nara.gov.* The material may be obtained from the National Security Division and the Cybersecurity and Infrastructure Security Agency (CISA), Mail Stop 0380, Department of Homeland Security, 245 Murray Lane, Washington, DC 20528–0380; *central@cisa.gov;* 888–282–0870; *www.cisa.gov/.*

§ 202.249 Sensitive personal data.

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

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

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

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

(3) Personal communications; and

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

§ 202.250 Special Administrative Region of Hong Kong.

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

§ 202.251 Special Administrative Region of Macau.

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

§ 202.252 Telecommunications service.

The term *telecommunications service* means the provision of voice and data communications services regardless of format or mode of delivery, including communications services delivered over cable, Internet Protocol, wireless, fiber, or other transmission mechanisms, as well as arrangements for network interconnection, transport, messaging, routing, or international voice, text, and data roaming.

§ 202.253 Transaction.

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

§ 202.254 Transfer.

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

§ 202.255 United States.

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

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

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

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

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

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

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

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

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

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

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

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

(2) [Reserved]

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

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

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

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

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

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

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

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

(A) Date of known or suspected violation;

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

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

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

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

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

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

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

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

(c) *Examples*—(1) *Example 1.* A U.S. business knowingly enters into an agreement to sell bulk human genomic data to a European business that is not a covered person. The U.S. business is required to include in that agreement a limitation on the European business' right to resell or otherwise engage in a covered data transaction involving data brokerage of that data to a country of concern or covered person. Otherwise, the agreement would be a prohibited transaction.

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

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

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

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

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

(a) *Prohibition.* Any transaction on or after the effective date that has the purpose of evading or avoiding, causes a violation of, or attempts to violate any of the prohibitions set forth in this part is prohibited. Any conspiracy formed to violate the prohibitions set forth in this part is prohibited.

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

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

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

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

(5) *Example 5.* A U.S. online gambling company uses an artificial intelligence algorithm to analyze collected bulk covered personal identifiers to identify users based on impulsivity for targeted advertising. The algorithm is trained on bulk covered personal identifiers and may reveal that raw data. A U.S. subsidiary of a company headquartered in a country of concern knows that the algorithm can reveal the training data. For the purpose of evasion, the U.S. subsidiary licenses the derivative algorithm from the U.S. online gambling company for the purpose of accessing bulk sensitive personal identifiers from the training data that would not otherwise be accessible to the parent company and shares the algorithm with the parent company so that the parent company can obtain the bulk covered personal identifiers. The U.S. subsidiary's licensing transaction with the parent company has the purpose of evading the regulations and is prohibited.

§ 202.305 Knowingly directing prohibited or restricted transactions.

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

applicable requirements under this part, if engaged in by a U.S. person.

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

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

(3) *Example 3.* A U.S. person is employed at a U.S.-headquartered multinational company that has a foreign affiliate that is not a covered person. The U.S. person instructs the U.S. company's compliance unit to change (or approve changes to) the operating policies and procedures of the foreign affiliate with the specific purpose of allowing the foreign affiliate to undertake covered data transactions that would be prohibited if performed by a 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 (as defined by § 202.408) required by this subpart D and all other applicable requirements under this part.

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

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

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

not authorized and thus is a prohibited transaction.

(3) *Example 3.* A U.S. person engages in a vendor agreement involving bulk U.S. sensitive personal data with a foreign person who is not a covered person. The foreign person then employs an individual who is a covered person and grants them access to bulk U.S. sensitive personal data without the U.S. person's knowledge or direction. There is no covered data transaction between the U.S. person and the covered person, and there is no indication that the parties engaged in these transactions with the purpose of evading the regulations (such as the U.S. person having knowingly directed the foreign person's employment agreement with the covered person or the parties knowingly structuring a prohibited transaction into these multiple transactions with the purpose of evading the prohibition). As a result, neither the vendor agreement nor the employment agreement would be a restricted transaction.

§ 202.402 [Reserved]

Subpart E—Exempt Transactions

§ 202.501 Personal communications.

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

§ 202.502 Information or informational materials.

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

§ 202.503 Travel.

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

§ 202.504 Official business of the United States Government.

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

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

(2) *Example 2.* A U.S. research institution receives a Federal grant to conduct human genomic research on U.S. and foreign persons. The Federal grant directs the U.S. research institution to publicize the results of its research, including the underlying human genomic data, via an internet-accessible database open to public health researchers with valid log-in credentials who pay a small annual fee to access the database, including covered persons primarily resident in a country of concern. The Federal grant does not cover the full costs of the authorized human genomic research or creation and publication of the database. The U.S. research institution obtains funds from private institutions and donors to fund the remaining costs. The human genomic research authorized by the Federal grant and publication of the database at the direction of the Federal grant would constitute a ''transaction[ ] conducted pursuant to a grant, contract, or other agreement entered into with the United States Government.'' The U.S. research institution must still comply with any requirements or prohibitions on sharing bulk U.S. sensitive personal data with countries of concern or covered persons required by the Federal grantmaker.

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

§ 202.505 Financial services.

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

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

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

(3) An activity that is ''financial in nature or incidental to such financial activity'' or ''complementary to a financial activity,'' section (k)(1), as set forth in section (k)(4) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)(4)) and rules and regulations and written interpretations of the Board of Governors of the Federal Reserve System thereunder;

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

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

payment-related loyalty point program administration); and

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

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

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

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

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

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

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

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

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

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

(10) *Example 10.* A U.S. financial services provider operates a foreign branch in a country of concern and provides financial services to U.S. persons living within the country of concern. The financial services provider receives a lawful request from the regulator in the country of concern to review the financial activity conducted in the country, which includes providing access to the bulk U.S. sensitive personal data of U.S. persons resident in the country or U.S. persons conducting transactions through the foreign branch. The financial services provider is also subject to ongoing and routine reporting requirements from various regulators in the country of concern. Responding to the regulator's request, including providing access to this bulk U.S. sensitive personal data, is ordinarily incident to the provision of financial services and is exempt.

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

(12) *Example 12.* A U.S. company provides wealth-management services and collects bulk personal financial data on its U.S. clients. The U.S. company appoints a citizen of a country of concern, who is located in a country of concern, to its board of directors. In connection with the board's data security and cybersecurity responsibilities, the director could compel company personnel or influence company policies or practices to provide the director access to the underlying bulk personal financial data the company collects on its U.S. clients. The appointment of the director, who is a covered person, is a restricted

employment agreement and is not exempt because the board member does not need to access, and in normal circumstances would not be able to access, the bulk financial data to perform his or her responsibilities. The board member's access to the bulk personal financial data is not ordinarily incident to the U.S. company's provision of wealth-management services.

§ 202.506 Corporate group transactions.

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

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

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

(i) Human resources;

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

(iii) Paying business taxes or fees;

(iv) Obtaining business permits or licenses;

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

(vi) Risk management;

(vii) Business-related travel;

(viii) Customer support;

(ix) Employee benefits; and

(x) Employees' internal and external communications.

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

(2) *Example 2.* A U.S. company aggregates bulk personal financial data. The U.S. company has a subsidiary that is a covered person because it is headquartered in a country of concern. The subsidiary is subject to the country of concern's national security laws requiring it to cooperate with and assist the country's intelligence services. The exemption for corporate group transactions would not apply to the U.S. parent's grant of a license to the subsidiary to access the parent's databases containing the bulk personal financial data for the purpose of complying with a request or order by the country of concern under those national security laws to provide access to that data because granting of such a license is not ordinarily incident to and part of administrative or ancillary business operations.

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

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

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

(6) *Example 6.* A U.S. financial services provider has a subsidiary located in a country of concern. Customers of the U.S. company conduct financial transactions in the country of concern, and customers of the foreign subsidiary conduct financial transactions in the United States. To perform customer service functions related to these financial transactions, the foreign subsidiary accesses bulk U.S. sensitive personal data—specifically, personal financial data. The corporate group transactions exemption would apply to the foreign subsidiary's access to the personal financial data under these circumstances because it is ordinarily incident to and part of the provision of customer support. The foreign subsidiary's access to the personal financial data would also be covered by the financial services exemption.

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

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

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

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

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

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

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

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

(7) Article 25 of the Agreement Between the Government of the United States of America and the Government of the People's Republic of China for the Avoidance of Double Taxation and the Prevention of Tax Evasion with Respect to Taxes on Income (1987);

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

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

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

Technology of Medicine and Public Health (2013);

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

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

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

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

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

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

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

(2) The Global Influenza Surveillance and Response System.

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

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

(2) [Reserved]

§ 202.508 Investment agreements subject to a CFIUS action.

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

(b) *Examples*—(1) *Example 1.* A U.S. software provider is acquired in a CFIUS covered transaction by a foreign entity in which the transaction parties sign a mitigation agreement with CFIUS. The agreement has provisions governing the acquirer's ability to access the data of the U.S. software provider and their customers. The mitigation agreement contains a provision stating that it is a CFIUS action for purposes of this part. Before the effective date of the CFIUS mitigation agreement, the investment agreement is not subject to a CFIUS action and remains subject to these regulations to the extent otherwise applicable. Beginning on the effective date of the CFIUS mitigation agreement, the investment agreement is subject to a CFIUS action and 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, D, J, and K (other than § 202.1102 and § 202.1104) of this part do not apply to data transactions, other than those involving data brokerage, to the extent that they are ordinarily incident to and part of the provision of telecommunications services.

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

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

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

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

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

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

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

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

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

(2) *Example 2.* Same as Example 1, except the regulatory entity in the country of concern requires that the data be de-anonymized. The transfer of data is not exempt under this section, because the data includes sensitive personal data that is identified to an individual.

(3) *Example 3.* Same as Example 1, except country of concern law requires foreign pharmaceutical companies to submit regulatory approval data using (1) a registered agent who primarily resides in the country of concern, (2) a country of concern incorporated subsidiary, or (3) an employee located in a country of concern. The U.S. pharmaceutical company enters into a vendor agreement with a registered agent in the country of concern to submit the regulatory approval data to the country of concern regulator. The U.S. pharmaceutical company provides to the registered agent only the regulatory approval data the U.S. pharmaceutical company intends the registered agent to submit to the country of concern regulator. The transaction with the registered agent is exempt, because it is necessary to obtain approval to market the drug in a country

of concern. The U.S. pharmaceutical company must comply with the recordkeeping and reporting requirements set forth in §§ 202.1101(a) and 202.1102 with respect to such transaction, however.

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

(5) *Example 5.* A U.S. pharmaceutical company has obtained regulatory approval to market a new drug in a country of concern. The country of concern regulator requires the U.S. pharmaceutical company to submit de-identified sensitive personal data collected as part of the company's post-marketing product surveillance activities to assess the safety and efficacy of the drug to the country of concern regulator via a country of concern registered agent to maintain the U.S. pharmaceutical company's authorization to market the drug. Sharing the de-identified sensitive personal data with the country of concern regulator via the country of concern registered agent to maintain marketing authorization is exempt from the prohibitions and restrictions in subparts C and D of this part.

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

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

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

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

(2) Ordinarily incident to and part of the collection or processing of clinical care data indicating real-world performance or safety of products, or the collection or processing of post-marketing surveillance data (including pharmacovigilance and post-marketing safety monitoring), and necessary to support or maintain authorization by the FDA, provided the data is de-identified or pseudonymized consistent with the standards of 21 CFR 314.80.

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

Subpart F—Determination of Countries of Concern

§ 202.601 Determination of countries of concern.

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

(1) China;

(2) Cuba;

(3) Iran;

(4) North Korea;

(5) Russia; and

(6) Venezuela.

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

Subpart G—Covered Persons

§ 202.701 Designation of covered persons.

(a) *Designations.* The Attorney General may designate any person as a covered person for purposes of this part if, after consultation with the Department of State and any other agencies as the Attorney General deems appropriate, the Attorney General determines the person meets any of the 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 H, or otherwise issued by the Department, authorizes or validates any transaction effected prior to the issuance of such license or other authorization, unless specifically provided for in such license or authorization.

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

(3) Any license authorizing or validating any transaction that is prohibited under or otherwise subject to this part has the effect of removing or 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 I were accurate and complete and to the extent the disclosures continue accurately and completely to reflect circumstances after the date of the issuance of the advisory opinion. An advisory opinion will not restrict enforcement actions by any agency other than the Department of Justice. It will not affect a requesting party's obligations to any other agency or under any statutory or regulatory provision other than those specifically discussed in the advisory opinion.

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

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

Subpart J—Due Diligence and Audit Requirements

§ 202.1001 Due diligence for restricted transactions.

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

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

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

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

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

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

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

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

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

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

§ 202.1002 Audits for restricted transactions.

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

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

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

(2) Must be independent; and

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

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

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

(e) *Scope.* The audit must:

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

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

(3) Examine relevant records required under § 202.1101;

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

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

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

(2) The audit report must:

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

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

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

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

(v) Describe any instances in which the security requirements failed or were otherwise not effective in mitigating the risk of access to government-related data or bulk U.S. sensitive personal data by a country of concern or covered person; and

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

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

Subpart K—Reporting and Recordkeeping Requirements

§ 202.1101 Records and recordkeeping requirements.

(a) *Records.* Except as otherwise provided, U.S. persons engaging in any transaction subject to the provisions of this part shall keep a full and accurate record of each such transaction engaged

in, and such record shall be available for examination for at least 10 years after the date of such transaction.

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

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

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

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

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

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

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

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

(5) Documentation of the method of data transfer;

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

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

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

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

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

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

§ 202.1102 Reports to be furnished on demand.

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

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

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

§ 202.1103 Annual reports.

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

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

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

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

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

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

(i) The date of the transaction;

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

(iii) The method of data transfer; and

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

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

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

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

§ 202.1104 Reports on rejected prohibited transactions.

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

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

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

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

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

(i) The date the transaction was rejected;

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

(iii) The method of data transfer;

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

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

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

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

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

§ 202.1201 Procedures.

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

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

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

(d) *Certification.* If the submitting party is an individual, the submission must be signed by the individual or the individual's attorney. If the submitting party is not an individual, the submission must be signed on behalf of each submitting party by an officer, director, a person performing the functions of an officer or a director of, or an attorney for, the submitting party. Annual reports submitted pursuant to § 202.1103, and reports on rejected transactions submitted pursuant to § 202.1104, 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.

(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.

(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.

TABLE 1 TO § 202.1401

Area ID	*Latitude/longitude coordinates of geofenced areas*			
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.
9	39.273162771, −76.362684384.	39.508996774, −76.362684384.	39.508996774, −76.049235582.	39.273162771, −76.049235582.
10	39.0258436940001, −76.9680962199999.	39.0402111820001, −76.9680962199999.	39.0402111820001, −76.9506770369999.	39.0258436940001, −76.9506770369999.
11	20.7457155230001, −156.440726997.	20.7494410490001, −156.440726997.	20.7494410490001, −156.431116699.	20.7457155230001, −156.431116699.
12	38.8805363480001, −77.1090209989999.	38.8811994730001, −77.1090209989999.	38.8811994730001, −77.1082027119999.	38.8805363480001, −77.1082027119999.
13	32.765632877, −97.460085871.	32.786292692, −97.460085871.	32.786292692, −97.445002478.	32.765632877, −97.445002478.
14	34.602177924, −118.126219217.	34.652496869, −118.126219217.	34.652496869, −118.040871203.	34.602177924, −118.040871203.
15	32.0905440820001, −110.959444035.	32.1053229630001, −110.959444035.	32.1053229630001, −110.922377001.	32.0905440820001, −110.922377001.
16	33.8999448750001, −84.540445929.	33.9364828150001, −84.540445929.	33.9364828150001, −84.511508719.	33.8999448750001, −84.511508719.
17	36.6657671500001, −76.163567934.	36.7187899800001, −76.163567934.	36.7187899800001, −76.098012048.	36.6657671500001, −76.098012048.
18	27.8761052880001, −98.061583281.	27.9157840450001, −98.061583281.	27.9157840450001, −98.0214386.	27.8761052880001, −98.0214386.
19	21.3545686960001, −157.926772605.	21.3700858780001, −157.926772605.	21.3700858780001, −157.89962502.	21.3545686960001, −157.89962502.
20	39.529701323, −78.871120656.	39.566862548, −78.871120656.	39.566862548, −78.819110448.	39.529701323, −78.819110448.
21	31.227908115, −85.654625655.	31.235020282, −85.654625655.	31.235020282, −85.646160343.	31.227908115, −85.646160343.
22	45.0576284000001, −83.5785134019999.	45.0972929400001, −83.5785134019999.	45.0972929400001, −83.5582903029999.	45.0576284000001, −83.5582903029999.
23	34.6379009080001, −99.303633301.	34.6889874940001, −99.303633301.	34.6889874940001, −99.25506291.	34.6379009080001, −99.25506291.
24	32.6375106470001, −117.168353987.	32.6816990190001, −117.168353987.	32.6816990190001, −117.138279193.	32.6375106470001, −117.138279193.
25	32.666935251, −117.172352209.	32.675675627, −117.172352209.	32.675675627, −117.163035197.	32.666935251, −117.163035197.
26	13.5479750120001, 144.840656045.	13.6479224930001, 144.840656045.	13.6479224930001, 144.956626971.	13.5479750120001, 144.956626971.
27	33.610199773, −86.013461889.	33.688770568, −86.013461889.	33.688770568, −85.910594886.	33.610199773, −85.910594886.
28	27.6372285040001, −81.364060357.	27.6776476600001, −81.364060357.	27.6776476600001, −81.326061341.	27.6372285040001, −81.326061341.
29	38.869169115, −77.079135005.	38.887908934, −77.079135005.	38.887908934, −77.058113411.	38.869169115, −77.058113411.
30	38.865964869, −77.081320445.	38.869010908, −77.081320445.	38.869010908, −77.07688713	38.865964869, −77.07688713.
31	30.268965988, −97.74101039	30.26898402, −97.74101039	30.26898402, −97.74098961	30.268965988, −97.74098961.
32	28.585892605, −81.197868843.	28.58638835, −81.197868843	28.58638835, −81.197094434	28.585892605, −81.197094434.
33	35.9939351130001, −78.8988567119999.	35.9939531280001, −78.8988567119999.	35.9939531280001, −78.8988345369999.	35.9939351130001, −78.8988345369999.
34	35.290658975, −86.1900228969999.	35.448152643, −86.1900228969999.	35.448152643, −85.9565678559999.	35.290658975, −85.9565678559999.
35	39.668741192, −74.486379079.	39.735566472, −74.486379079.	39.735566472, −74.38985998	39.668741192, −74.38985998.
36	27.5433418430001, −81.440651203.	27.7481014920001, −81.440651203.	27.7481014920001, −81.140127987.	27.5433418430001, −81.140127987.
37	43.329662741, −89.768817729.	43.3804415840001, −89.768817729.	43.3804415840001, −89.704814972.	43.329662741, −89.704814972.
38	32.7213462890001, −117.147436521.	32.7304327800001, −117.147436521.	32.7304327800001, −117.142819245.	32.7213462890001, −117.142819245.
39	44.810736596, −68.845190583.	44.824436067, −68.845190583.	44.824436067, −68.817759555.	44.810736596, −68.817759555.
40	30.378935891, −87.651017989.	30.406043932, −87.651017989.	30.406043932, −87.616693181.	30.378935891, −87.616693181.

TABLE 1 TO § 202.1401—Continued

Area ID				
41	32.460689648, −93.692932035.	32.533707929, −93.692932035.	32.533707929, −93.531044113.	32.460689648, −93.531044113.
42	42.1637746650001, −72.721474954.	42.1737587120001, −72.721474954.	42.1737587120001, −72.713127559.	42.1637746650001, −72.713127559.
43	32.234848137, −114.563241999.	32.74030585, −114.563241999.	32.74030585, −113.597922719.	32.234848137, −113.597922719.
44	32.8717587680001, −112.742209944.	32.9055316810001, −112.742209944.	32.9055316810001, −112.715649106.	32.8717587680001, −112.715649106.
45	70.118081036, −143.649422567.	70.13677672, −143.649422567.	70.13677672, −143.549196508.	70.118081036, −143.549196508.
46	39.0718274430001, −121.477278056.	39.1737524000001, −121.477278056.	39.1737524000001, −121.321123307.	39.0718274430001, −121.321123307.
47	21.3446919420001, −157.715961149.	21.3801950850001, −157.715961149.	21.3801950850001, −157.704152283.	21.3446919420001, −157.704152283.
48	39.320337941, −80.27238984	39.332562421, −80.27238984	39.332562421, −80.257518209.	39.320337941, −80.257518209.
49	64.3151851490001, −146.65232338.	64.3202659380001, −146.65232338.	64.3202659380001, −146.642748991.	64.3151851490001, −146.642748991.
50	33.564586567, −86.7593074919999.	33.577571506, −86.7593074919999.	33.577571506, −86.749335831.	33.564586567, −86.749335831.
51	33.979025715, −77.920042096.	33.98353888, −77.920042096	33.98353888, −77.911945012	33.979025715, −77.911945012.
52	37.6569067660001, −84.2697493539999.	37.7403075720001, −84.2697493539999.	37.7403075720001, −84.1739063399999.	37.6569067660001, −84.1739063399999.
53	43.549701982, −116.23995646.	43.565222364, −116.23995646.	43.565222364, −116.203444555.	43.549701982, −116.203444555.
54	41.928394165, −72.706470888.	41.940084218, −72.706470888.	41.940084218, −72.6950519379999.	41.928394165, −72.6950519379999.
55	41.5399982100001, −81.628180911.	41.5451316070001, −81.628180911.	41.5451316070001, −81.623066892.	41.5399982100001, −81.623066892.
56	38.259480861, −119.65128069.	38.488443466, −119.65128069.	38.488443466, −119.46086144.	38.259480861, −119.46086144.
57	32.7116821270001, −117.172842204.	32.7155456210001, −117.172842204.	32.7155456210001, −117.171235129.	32.7116821270001, −117.171235129.
58	40.5796208020001, −73.881158344.	40.5851822330001, −73.881158344.	40.5851822330001, −73.875044844.	40.5796208020001, −73.875044844.
59	31.3815422060001, −85.978073125.	31.3912525150001, −85.978073125.	31.3912525150001, −85.96646119.	31.3815422060001, −85.96646119.
60	39.6792307960001, −104.791155246.	39.7256386980001, −104.791155246.	39.7256386980001, −104.732681808.	39.6792307960001, −104.732681808.
61	44.465375824, −73.165872108.	44.481431105, −73.165872108.	44.481431105, −73.138589437.	44.465375824, −73.138589437.
62	18.246447926, −65.580288041.	18.250653732, −65.580288041.	18.250653732, −65.57513189	18.246447926, −65.57513189.
63	31.2653802660001, −85.730112602.	31.2900770820001, −85.730112602.	31.2900770820001, −85.701272345.	31.2653802660001, −85.701272345.
64	13.488847714, 144.8237902 ...	13.650804937, 144.8237902 ...	13.650804937, 144.882806074	13.488847714, 144.882806074.
65	41.613354353, −93.9831494479999.	42.134619451, −93.9831494479999.	42.134619451, −93.625230214.	41.613354353, −93.625230214.
66	34.6199016640001, −84.1105367119999.	34.6357614130001, −84.1105367119999.	34.6357614130001, −84.0950752379999.	34.6199016640001, −84.0950752379999.
67	44.5103232180001, −85.0727276169999.	44.8976058610001, −85.0727276169999.	44.8976058610001, −84.4513643499999.	44.5103232180001, −84.4513643499999.
68	35.0011406840001, −79.523939868.	35.0683094360001, −79.523939868.	35.0683094360001, −79.442653881.	35.0011406840001, −79.442653881.
69	32.641816556, −116.466773316.	32.70380767, −116.466773316.	32.70380767, −116.419479903.	32.641816556, −116.419479903.
70	32.707519441, −116.520980841.	32.714794633, −116.520980841.	32.714794633, −116.509578866.	32.707519441, −116.509578866.
71	35.1488975340001, −111.913136629.	35.2519317510001, −111.913136629.	35.2519317510001, −111.772220092.	35.1488975340001, −111.772220092.
72	35.688234999, −120.85951023.	35.893098334, −120.85951023.	35.893098334, −120.711509738.	35.688234999, −120.711509738.
73	30.91049165, −89.245591473	31.215207751, −89.245591473.	31.215207751, −88.825853545.	30.91049165, −88.825853545.
74	40.3878151230001, −112.116737638.	40.4646164020001, −112.116737638.	40.4646164020001, −111.91331559.	40.3878151230001, −111.91331559.
75	34.40563345, −103.337070541.	34.412489823, −103.337070541.	34.412489823, −103.319797859.	34.40563345, −103.319797859.
76	34.3614483640001, −103.354726446.	34.4053770780001, −103.354726446.	34.4053770780001, −103.295530382.	34.3614483640001, −103.295530382.

TABLE 1 TO § 202.1401—Continued

Area ID				
77	28.410293461, −80.611521457.	28.569239286, −80.611521457.	28.569239286, −80.525040895.	28.410293461, −80.525040895.
78	58.6207566940001, −162.088477025.	58.6671382160001, −162.088477025.	58.6671382160001, −162.051955173.	58.6207566940001, −162.051955173.
79	39.843911672, −89.673153301.	39.853707959, −89.673153301.	39.853707959, −89.664434939.	39.843911672, −89.664434939.
80	40.1998354450001, −77.1813079679999.	40.2155193840001, −77.1813079679999.	40.2155193840001, −77.1567188819999.	40.1998354450001, −77.1567188819999.
81	48.720965666, −97.91415126	48.732224729, −97.91415126	48.732224729, −97.892530954.	48.720965666, −97.892530954.
82	30.3692267820001, −89.145003244.	30.3839136300001, −89.145003244.	30.3839136300001, −89.1029689419999.	30.3692267820001, −89.1029689419999.
83	34.133132274, −119.113804625.	34.1468546850001, −119.113804625.	34.1468546850001, −119.107499465.	34.133132274, −119.107499465.
84	35.2130798650001, −80.93434288.	35.2209434880001, −80.93434288.	35.2209434880001, −80.924747233.	35.2130798650001, −80.924747233.
85	37.268469865, −76.6497831579999.	37.300168225, −76.6497831579999.	37.300168225, −76.5808454679999.	37.268469865, −76.5808454679999.
86	38.652772446, −76.537514883.	38.665190459, −76.537514883.	38.665190459, −76.526755785.	38.652772446, −76.526755785.
87	38.730266928, −104.854175709.	38.748479779, −104.854175709.	38.748479779, −104.830998169.	38.730266928, −104.830998169.
88	41.1585808, −104.827282882	41.163962628, −104.827282882.	41.163962628, −104.811583526.	41.1585808, −104.811583526.
89	33.0433918000001, −115.769002927.	33.561860554, −115.769002927.	33.561860554, −114.937048224.	33.0433918000001, −114.937048224.
90	64.256937909, −149.271311872.	64.318532807, −149.271311872.	64.318532807, −149.078782527.	64.256937909, −149.078782527.
91	48.0181544170001, −122.749058066.	48.0882406420001, −122.749058066.	48.0882406420001, −122.699833714.	48.0181544170001, −122.699833714.
92	55.260399471, −162.892009844.	55.266039599, −162.892009844.	55.266039599, −162.882133146.	55.260399471, −162.882133146.
93	32.9238514580001, −88.597781493.	33.6613396510001, −88.597781493.	33.6613396510001, −88.419408536.	32.9238514580001, −88.419408536.
94	42.2857517910001, −71.366797532.	42.2934966590001, −71.366797532.	42.2934966590001, −71.355575286.	42.2857517910001, −71.355575286.
95	30.396955129, −87.301358539.	30.41034727, −87.301358539	30.41034727, −87.278142462	30.396955129, −87.278142462.
96	36.8832992170001, −76.3808126719999.	36.8943868090001, −76.3808126719999.	36.8943868090001, −76.3390713729999.	36.8832992170001, −76.3390713729999.
97	36.4941214200001, −115.88042321.	36.7385429400001, −115.88042321.	36.7385429400001, −115.4868387.	36.4941214200001, −115.4868387.
98	21.299764458, −158.073065748.	21.327294536, −158.073065748.	21.327294536, −158.044610628.	21.299764458, −158.044610628.
99	36.779547069, −119.702471155.	36.782099199, −119.702471155.	36.782099199, −119.701514522.	36.779547069, −119.701514522.
100	42.15393814, −70.9374754149999.	42.158515225, −70.9374754149999.	42.158515225, −70.9301741339999.	42.15393814, −70.9301741339999.
101	48.4214595020001, −117.41300542.	48.5515751880001, −117.41300542.	48.5515751880001, −117.35926532.	48.4214595020001, −117.35926532.
102	26.091587869, −80.111818708.	26.092584016, −80.111818708.	26.092584016, −80.108205835.	26.091587869, −80.108205835.
103	35.6459372400001, −75.991669019.	35.7768890170001, −75.991669019.	35.7768890170001, −75.771652698.	35.6459372400001, −75.771652698.
104	32.1193109110001, −110.909314221.	32.1962087390001, −110.909314221.	32.1962087390001, −110.789766372.	32.1193109110001, −110.789766372.
105	37.408487704, −77.453738162.	37.439266805, −77.453738162.	37.439266805, −77.435618651.	37.408487704, −77.435618651.
106	38.8781991000001, −77.109040482.	38.8792949460001, −77.109040482.	38.8792949460001, −77.108174294.	38.8781991000001, −77.108174294.
107	40.1972506380001, −76.853865245.	40.2226551520001, −76.853865245.	40.2226551520001, −76.8221857039999.	40.1972506380001, −76.8221857039999.
108	39.974582163, −82.913383443.	39.985122185, −82.913383443.	39.985122185, −82.884325098.	39.974582163, −82.884325098.
109	41.537901628, −93.674402705.	41.549978514, −93.674402705.	41.549978514, −93.657102163.	41.537901628, −93.657102163.
110	30.40946552, −86.500613385	30.412738745, −86.500613385.	30.412738745, −86.4971744769999.	30.40946552, −86.4971744769999.
111	37.9630717110001, −122.027819871.	38.0227201040001, −122.027819871.	38.0227201040001, −121.939142028.	37.9630717110001, −121.939142028.
112	39.8839370650001, −75.190933843.	39.8984743260001, −75.190933843.	39.8984743260001, −75.16306509.	39.8839370650001, −75.16306509.

TABLE 1 TO § 202.1401—Continued

Area ID				
113	42.4914812000001, −83.046418438.	42.5026695230001, −83.046418438.	42.5026695230001, −83.037544269.	42.4914812000001, −83.037544269.
114	42.4694829900001, −71.691664547.	42.5765892500001, −71.691664547.	42.5765892500001, −71.603764233.	42.4694829900001, −71.603764233.
115	46.9314271700001, −67.8969077639999.	46.9342671660001, −67.8969077639999.	46.9342671660001, −67.8923200479999.	46.9314271700001, −67.8923200479999.
116	21.567863645, −158.21347981.	21.581952858, −158.21347981.	21.581952858, −158.180039671.	21.567863645, −158.180039671.
117	28.0671354250001, −98.778173769.	28.1245884970001, −98.778173769.	28.1245884970001, −98.685192869.	28.0671354250001, −98.685192869.
118	33.8969244250001, −84.542380856.	33.9367576460001, −84.542380856.	33.9367576460001, −84.495305955.	33.8969244250001, −84.495305955.
119	39.10595655, −75.494449085	39.152386899, −75.494449085.	39.152386899, −75.436634728.	39.10595655, −75.436634728.
120	24.568031467, −81.781745689.	24.585123807, −81.781745689.	24.585123807, −81.765170818.	24.568031467, −81.765170818.
121	32.674333394, −117.133765	32.692839739, −117.133765	32.692839739, −117.108967938.	32.674333394, −117.108967938.
122	46.8330442210001, −92.21102751.	46.8510308170001, −92.21102751.	46.8510308170001, −92.165423416.	46.8330442210001, −92.165423416.
123	32.3941914100001, −99.867572545.	32.4478988670001, −99.867572545.	32.4478988670001, −99.808678428.	32.3941914100001, −99.808678428.
124	52.7044712040001, 174.053643507.	52.7410254930001, 174.053643507.	52.7410254930001, 174.156518998.	52.7044712040001, 174.156518998.
125	34.762486344, −118.140763438.	35.017611389, −118.140763438.	35.017611389, −117.525081645.	34.762486344, −117.525081645.
126	30.381138945, −86.8509824239999.	30.405275435, −86.8509824239999.	30.405275435, −86.6331687359999.	30.381138945, −86.6331687359999.
127	30.6217855130001, −86.7554594279999.	30.6494843350001, −86.7554594279999.	30.6494843350001, −86.7303715759999.	30.6217855130001, −86.7303715759999.
128	27.0764966720001, −86.983116121.	30.7497294690001, −86.983116121.	30.7497294690001, −82.448862506.	27.0764966720001, −82.448862506.
129	64.6012802210001, −147.165786418.	64.7480079510001, −147.165786418.	64.7480079510001, −146.938371648.	64.6012802210001, −146.938371648.
130	36.8644398160001, −76.3344377989999.	36.8708429060001, −76.3344377989999.	36.8708429060001, −76.3299793119999.	36.8644398160001, −76.3299793119999.
131	29.5899224830001, −95.17474779.	29.6230511860001, −95.17474779.	29.6230511860001, −95.16633921.	29.5899224830001, −95.16633921.
132	44.112997566, −103.129144564.	44.176511165, −103.129144564.	44.176511165, −103.060660125.	44.112997566, −103.060660125.
133	31.325926945, −92.549004972.	31.34466339, −92.549004972	31.34466339, −92.532050872	31.325926945, −92.532050872.
134	39.4012000000001, −77.9954	39.4140000010001, −77.9954	39.4140000010001, −77.9708	39.4012000000001, −77.9708.
135	47.5887747180001, −117.693058242.	47.6428480860001, −117.693058242.	47.6428480860001, −117.623082729.	47.5887747180001, −117.623082729.
136	33.3291382400001, −117.313779432.	33.3984247810001, −117.313779432.	33.3984247810001, −117.249241913.	33.3291382400001, −117.249241913.
137	38.826363557, −118.950589204.	39.942237, −118.950589204	39.942237, −117.125199131	38.826363557, −117.125199131.
138	36.9206436430001, −76.324596591.	36.9225983950001, −76.324596591.	36.9225983950001, −76.321048116.	36.9206436430001, −76.321048116.
139	30.395125636, −81.633046236.	30.406669179, −81.633046236.	30.406669179, −81.613437212.	30.395125636, −81.613437212.
140	24.567441214, −81.801443736.	24.594738599, −81.801443736.	24.594738599, −81.79382837	24.567441214, −81.79382837.
141	38.9355059150001, −95.6866671779999.	38.9672269680001, −95.6866671779999.	38.9672269680001, −95.6739997489999.	38.9355059150001, −95.6739997489999.
142	32.7263297590001, −117.225651967.	32.7323354850001, −117.225651967.	32.7323354850001, −117.215769817.	32.7263297590001, −117.215769817.
143	41.4732485420001, −71.3429884129999.	41.4772592680001, −71.3429884129999.	41.4772592680001, −71.3354651549999.	41.4732485420001, −71.3354651549999.
144	38.6728683430001, −77.202015081.	38.7484680470001, −77.202015081.	38.7484680470001, −77.1209734769999.	38.6728683430001, −77.1209734769999.
145	39.855326909, −86.028620872.	39.864369447, −86.028620872.	39.864369447, −86.003845091.	39.855326909, −86.003845091.
146	31.7888139250001, −106.581474459.	32.6965880790001, −106.581474459.	32.6965880790001, −105.524846042.	31.7888139250001, −105.524846042.
147	18.4046924090001, −66.1341755349999.	18.4221096420001, −66.1341755349999.	18.4221096420001, −66.1054899209999.	18.4046924090001, −66.1054899209999.
148	36.5354833810001, −87.820914236.	36.7268240330001, −87.820914236.	36.7268240330001, −87.423400866.	36.5354833810001, −87.423400866.

TABLE 1 TO § 202.1401—Continued

Area ID				
149	38.418237328, −104.967064928.	38.765149965, −104.967064928.	38.765149965, −104.717754537.	38.418237328, −104.717754537.
150	30.7215072980001, −97.913021062.	31.3927951710001, −97.913021062.	31.3927951710001, −97.382600936.	30.7215072980001, −97.382600936.
151	21.277988357, −157.837039889.	21.28553417, −157.837039889.	21.28553417, −157.831141168.	21.277988357, −157.831141168.
152	39.428600294, −77.437471934.	39.450390568, −77.437471934.	39.450390568, −77.410819037.	39.428600294, −77.410819037.
153	39.0020859900001, −77.060006807.	39.0129141590001, −77.060006807.	39.0129141590001, −77.05003399.	39.0020859900001, −77.05003399.
154	39.0320227890001, −77.04385429.	39.0346693610001, −77.04385429.	39.0346693610001, −77.03866628.	39.0320227890001, −77.03866628.
155	44.010913031, −75.842125669.	44.256536804, −75.842125669.	44.256536804, −75.386367945.	44.010913031, −75.386367945.
156	33.274519335, −82.379611728.	33.440619771, −82.379611728.	33.440619771, −82.096232277.	33.274519335, −82.096232277.
157	33.6089633770001, −84.35154274.	33.6319158920001, −84.35154274.	33.6319158920001, −84.307486309.	33.6089633770001, −84.307486309.
158	63.9388112670001, −145.772613518.	64.0231208060001, −145.772613518.	64.0231208060001, −145.655809936.	63.9388112670001, −145.655809936.
159	37.213516865, −77.358595158.	37.298684924, −77.358595158.	37.298684924, −77.307488144.	37.213516865, −77.307488144.
160	40.604582683, −74.034049003.	40.613167841, −74.034049003.	40.613167841, −74.0206090659999.	40.604582683, −74.0206090659999.
161	31.434363842, −110.449131361.	31.686859773, −110.449131361.	31.686859773, −110.188946087.	31.434363842, −110.188946087.
162	35.7935092910001, −121.426498813.	36.1147194860001, −121.426498813.	36.1147194860001, −121.031600619.	35.7935092910001, −121.031600619.
163	35.082504812, −117.084003937.	35.627708795, −117.084003937.	35.627708795, −116.163545882.	35.082504812, −116.163545882.
164	33.9829769470001, −80.959251815.	34.0836392030001, −80.959251815.	34.0836392030001, −80.704124579.	33.9829769470001, −80.704124579.
165	30.921870988, −93.579998793.	31.490503162, −93.579998793.	31.490503162, −92.862745164.	30.921870988, −92.862745164.
166	37.78807672, −86.056877114	38.0073711200001, −86.056877114.	38.0073711200001, −85.747574551.	37.78807672, −85.747574551.
167	39.3284266840001, −94.949264706.	39.3922569280001, −94.949264706.	39.3922569280001, −94.880745646.	39.3284266840001, −94.880745646.
168	37.6037963470001, −92.2500513099999.	37.7999725520001, −92.2500513099999.	37.7999725520001, −92.0408380759999.	37.6037963470001, −92.0408380759999.
169	35.039462073, −79.38062969	35.274563988, −79.38062969	35.274563988, −78.901879671.	35.039462073, −78.901879671.
170	43.90284867, −90.765375865	44.159924233, −90.765375865.	44.159924233, −90.587856675.	43.90284867, −90.587856675.
171	39.071479147, −76.776616336.	39.130981819, −76.776616336.	39.130981819, −76.709232204.	39.071479147, −76.709232204.
172	40.2844597280001, −74.096750839.	40.3390552010001, −74.096750839.	40.3390552010001, −74.026249284.	40.2844597280001, −74.026249284.
173	37.000205414, −76.3170219039999.	37.035192566, −76.3170219039999.	37.035192566, −76.2925912169999.	37.000205414, −76.2925912169999.
174	32.2387118290001, −85.021200904.	32.5517604030001, −85.021200904.	32.5517604030001, −84.637054935.	32.2387118290001, −84.637054935.
175	31.314144049, −85.865695246.	31.505687537, −85.865695246.	31.505687537, −85.612193512.	31.314144049, −85.612193512.
176	39.0366899860001, −96.962729439.	39.3067854380001, −96.962729439.	39.3067854380001, −96.681803847.	39.0366899860001, −96.681803847.
177	21.3344869650001, −157.894073145.	21.3570876230001, −157.894073145.	21.3570876230001, −157.87189508.	21.3344869650001, −157.87189508.
178	42.203459073, −87.8100502569999.	42.216029281, −87.8100502569999.	42.216029281, −87.7987031449999.	42.203459073, −87.7987031449999.
179	34.637509069, −98.755961597.	34.768015017, −98.755961597.	34.768015017, −98.282396833.	34.637509069, −98.282396833.
180	35.247127112, −94.374048025.	35.345197662, −94.374048025.	35.345197662, −94.080609487.	35.247127112, −94.080609487.
181	31.8490945500001, −81.889069385.	32.1248422650001, −81.889069385.	32.1248422650001, −81.304927888.	31.8490945500001, −81.304927888.
182	63.495426454, −148.652607873.	64.877948104, −148.652607873.	64.877948104, −145.011700164.	63.495426454, −145.011700164.
183	38.018142733, −77.395133849.	38.2229469870001, −77.395133849.	38.2229469870001, −77.136746906.	38.018142733, −77.136746906.
184	35.4225141090001, −108.629517745.	35.5234010050001, −108.629517745.	35.5234010050001, −108.546488603.	35.4225141090001, −108.546488603.

TABLE 1 TO § 202.1401—Continued

Area ID				
185	66.558440788, −145.217198219.	66.562635721, −145.217198219.	66.562635721, −145.196865879.	66.558440788, −145.196865879.
186	41.131595797, −104.888175803.	41.201251583, −104.888175803.	41.201251583, −104.839386748.	41.131595797, −104.839386748.
187	40.8317168790001, −72.646569509.	40.8404590060001, −72.646569509.	40.8404590060001, −72.637878307.	40.8317168790001, −72.637878307.
188	36.7652210320001, −119.726849268.	36.7866408030001, −119.726849268.	36.7866408030001, −119.702290588.	36.7652210320001, −119.702290588.
189	39.046072102, −76.689705918.	39.068500337, −76.689705918.	39.068500337, −76.660214864.	39.046072102, −76.660214864.
190	42.9373147850001, −87.891735357.	42.9447209110001, −87.891735357.	42.9447209110001, −87.88532841.	42.9373147850001, −87.88532841.
191	40.6559953350001, −89.713436026.	40.6713177760001, −89.713436026.	40.6713177760001, −89.691898535.	40.6559953350001, −89.691898535.
192	42.297663631, −87.8562319869999.	42.303204758, −87.8562319869999.	42.303204758, −87.8518457849999.	42.297663631, −87.8518457849999.
193	42.0902179130001, −87.8412161049999.	42.0929537750001, −87.8412161049999.	42.0929537750001, −87.8329821559999.	42.0902179130001, −87.8329821559999.
194	31.410361906, −85.4658208399999.	31.419467447, −85.4658208399999.	31.419467447, −85.4610573259999.	31.410361906, −85.4610573259999.
195	33.422394339, −112.015046889.	33.427659719, −112.015046889.	33.427659719, −112.006740103.	33.422394339, −112.006740103.
196	31.4211524990001, −100.421423136.	31.4502936180001, −100.421423136.	31.4502936180001, −100.386562872.	31.4211524990001, −100.386562872.
197	41.5355012680001, −71.3460647429999.	41.5398354990001, −71.3460647429999.	41.5398354990001, −71.3433558969999.	41.5355012680001, −71.3433558969999.
198	47.921128756, −97.4238744209999.	48.00111753, −97.4238744209999.	48.00111753, −97.3251566139999.	47.921128756, −97.3251566139999.
199	32.7378756470001, −96.960057831.	32.7421326520001, −96.960057831.	32.7421326520001, −96.951545219.	32.7378756470001, −96.951545219.
200	47.471916874, −111.370342141.	47.482136373, −111.370342141.	47.482136373, −111.35856852.	47.471916874, −111.35856852.
201	38.935411516, −110.143618375.	38.983389468, −110.143618375.	38.983389468, −110.064497018.	38.935411516, −110.064497018.
202	40.629836335, −86.175582897.	40.6784136910001, −86.175582897.	40.6784136910001, −86.124933251.	40.629836335, −86.124933251.
203	30.404753499, −89.06446994	30.416012997, −89.06446994	30.416012997, −89.05803309	30.404753499, −89.05803309.
204	62.384524694, −145.202752458.	62.438701327, −145.202752458.	62.438701327, −145.108315	62.384524694, −145.108315.
205	43.0985925350001, −76.1175710329999.	43.1204055300001, −76.1175710329999.	43.1204055300001, −76.0811541549999.	43.0985925350001, −76.0811541549999.
206	42.449141119, −71.2922332959999.	42.477596104, −71.2922332959999.	42.477596104, −71.263228187.	42.449141119, −71.263228187.
207	32.728744878, −117.208959019.	32.730100028, −117.208959019.	32.730100028, −117.205155926.	32.728744878, −117.205155926.
208	44.220163461, −90.111781241.	44.249174018, −90.111781241.	44.249174018, −89.996184064.	44.220163461, −89.996184064.
209	38.229497861, −118.850468214.	38.675823329, −118.850468214.	38.675823329, −118.465402259.	38.229497861, −118.465402259.
210	46.9082501180001, −96.813335915.	46.9192707510001, −96.813335915.	46.9192707510001, −96.797905722.	46.9082501180001, −96.797905722.
211	21.530784666, −158.026158574.	21.541312201, −158.026158574.	21.541312201, −158.012928076.	21.530784666, −158.012928076.
212	21.4521601660001, −158.036478816.	21.4580696550001, −158.036478816.	21.4580696550001, −158.032403386.	21.4521601660001, −158.032403386.
213	31.1479145100001, −85.744240415.	31.1546432720001, −85.744240415.	31.1546432720001, −85.729933472.	31.1479145100001, −85.729933472.
214	41.0983339530001, −112.024399889.	41.1651189630001, −112.024399889.	41.1651189630001, −111.942395214.	41.0983339530001, −111.942395214.
215	32.7930228270001, −106.204383402.	33.0771885310001, −106.204383402.	33.0771885310001, −106.049512667.	32.7930228270001, −106.049512667.
216	36.4958650950001, −82.684996348.	36.5518898770001, −82.684996348.	36.5518898770001, −82.546522187.	36.4958650950001, −82.546522187.
217	32.828679521, −115.288498013.	32.846906967, −115.288498013.	32.846906967, −115.14568048.	32.828679521, −115.14568048.
218	25.4901310220001, −80.4045291039999.	25.5181528940001, −80.4045291039999.	25.5181528940001, −80.3779792709999.	25.4901310220001, −80.3779792709999.
219	39.446631245, −87.304009056.	39.458100621, −87.304009056.	39.458100621, −87.290668741.	39.446631245, −87.290668741.
220	31.3751890450001, −85.5828701299999.	31.3850761720001, −85.5828701299999.	31.3850761720001, −85.5773414419999.	31.3751890450001, −85.5773414419999.

TABLE 1 TO § 202.1401—Continued

Area ID				
221	31.9832369490001, −81.198805141.	32.0349005460001, −81.198805141.	32.0349005460001, −81.113375475.	31.9832369490001, −81.113375475.
222	30.406119645, −86.74211065	30.45486409, −86.74211065	30.45486409, −86.655360926	30.406119645, −86.655360926.
223	32.5545594160001, −117.133035356.	32.5724338440001, −117.133035356.	32.5724338440001, −117.089509557.	32.5545594160001, −117.089509557.
224	65.9646785140001, −153.812691683.	66.1009999220001, −153.812691683.	66.1009999220001, −153.662067587.	65.9646785140001, −153.662067587.
225	38.435308005, −85.627248303.	38.4668353, −85.627248303	38.4668353, −85.584713152	38.435308005, −85.584713152.
226	40.7516430220001, −91.325065862.	40.8294821280001, −91.325065862.	40.8294821280001, −91.178786412.	40.7516430220001, −91.178786412.
227	32.311624454, −90.0879237459999.	32.328439256, −90.0879237459999.	32.328439256, −90.0778932449999.	32.311624454, −90.0778932449999.
228	30.402512915, −81.628884649.	30.408229141, −81.628884649.	30.408229141, −81.613589029.	30.402512915, −81.613589029.
229	29.9570817420001, −81.972797144.	30.4921986090001, −81.972797144.	30.4921986090001, −81.69382023.	29.9570817420001, −81.69382023.
230	38.8109873670001, −85.4822157569999.	39.0601368300001, −85.4822157569999.	39.0601368300001, −85.3594923629999.	38.8109873670001, −85.3594923629999.
231	48.1670940830001, −121.958243024.	48.2248098330001, −121.958243024.	48.2248098330001, −121.887559225.	48.1670940830001, −121.887559225.
232	43.5700133340001, −96.7515566289999.	43.5962111540001, −96.7515566289999.	43.5962111540001, −96.7347550689999.	43.5700133340001, −96.7347550689999.
233	38.823559833, −77.026428621.	38.867319001, −77.026428621.	38.867319001, −77.002855219.	38.823559833, −77.002855219.
234	38.7822985190001, −76.90343143.	38.829021577, −76.90343143	38.829021577, −76.8490210659999.	38.7822985190001, −76.8490210659999.
235	41.6372929940001, −70.5993199659999.	41.7708974620001, −70.5993199659999.	41.7708974620001, −70.4886883249999.	41.6372929940001, −70.4886883249999.
236	32.873792952, −81.104787366.	33.621879998, −81.104787366.	33.621879998, −79.90958174	32.873792952, −79.90958174.
237	61.1317682310001, −149.879980832.	61.4090492570001, −149.879980832.	61.4090492570001, −149.522914627.	61.1317682310001, −149.522914627.
238	37.063373746, −76.627940713.	37.182586941, −76.627940713.	37.182586941, −76.336599693.	37.063373746, −76.336599693.
239	45.8002376150001, −122.802079191.	47.2187487550001, −122.802079191.	47.2187487550001, −119.30029009.	45.8002376150001, −119.30029009.
240	39.9443860000001, −74.661412648.	40.0586108630001, −74.661412648.	40.0586108630001, −74.304547511.	39.9443860000001, −74.304547511.
241	38.8611352610001, −77.084491842.	38.8880351040001, −77.084491842.	38.8880351040001, −77.013817583.	38.8611352610001, −77.013817583.
242	21.2966123480001, −158.17382288.	21.6863899190001, −158.17382288.	21.6863899190001, −157.850223188.	21.2966123480001, −157.850223188.
243	29.346205018, −98.690308725.	29.893089367, −98.690308725.	29.893089367, −97.884281333.	29.346205018, −97.884281333.
244	36.892714836, −76.1925524759999.	36.932892732, −76.1925524759999.	36.932892732, −75.9873603089999.	36.892714836, −75.9873603089999.
245	37.8190118270001, −75.514689614.	37.9512715100001, −75.514689614.	37.9512715100001, −75.413609963.	37.8190118270001, −75.413609963.
246	40.6939221220001, −84.148196529.	40.7086310680001, −84.148196529.	40.7086310680001, −84.127525454.	40.6939221220001, −84.127525454.
247	41.3409958870001, −88.082958084.	41.3733639960001, −88.082958084.	41.3733639960001, −88.046036417.	41.3409958870001, −88.046036417.
248	41.4073674850001, −88.187831293.	41.4365859010001, −88.187831293.	41.4365859010001, −88.107459928.	41.4073674850001, −88.107459928.
249	21.560298554, −158.266932035.	21.572360392, −158.266932035.	21.572360392, −158.237835914.	21.560298554, −158.237835914.
250	21.6027392400001, −158.033515202.	21.6936355750001, −158.033515202.	21.6936355750001, −157.95298898.	21.6027392400001, −157.95298898.
251	22.035974347, −159.75916373.	22.042080758, −159.75916373.	22.042080758, −159.750865139.	22.035974347, −159.750865139.
252	20.0291620130001, −155.834320072.	20.0374297880001, −155.834320072.	20.0374297880001, −155.823440805.	20.0291620130001, −155.823440805.
253	30.398126636, −88.9508689469999.	30.420139346, −88.9508689469999.	30.420139346, −88.896527048.	30.398126636, −88.896527048.
254	36.7153178120001, −98.128361282.	36.7547185190001, −98.128361282.	36.7547185190001, −98.110051089.	36.7153178120001, −98.110051089.
255	60.558793666, −151.257835885.	60.560759837, −151.257835885.	60.560759837, −151.254274297.	60.558793666, −151.254274297.
256	19.4318712580001, −155.27720251.	19.4367646340001, −155.27720251.	19.4367646340001, −155.271614951.	19.4318712580001, −155.271614951.

TABLE 1 TO § 202.1401—Continued

Area ID				
257	58.638365343, −156.693447262.	58.708746999, −156.693447262.	58.708746999, −156.459187473.	58.638365343, −156.459187473.
258	42.1444655070001, −121.753628091.	42.1707914760001, −121.753628091.	42.1707914760001, −121.727677654.	42.1444655070001, −121.727677654.
259	21.4148860290001, −158.014284187.	21.4580033840001, −158.014284187.	21.4580033840001, −157.991853913.	21.4148860290001, −157.991853913.
260	34.9471711320001, −106.613226109.	35.0673284870001, −106.613226109.	35.0673284870001, −106.360768374.	34.9471711320001, −106.360768374.
261	57.816486609, −152.341066882.	57.826001907, −152.341066882.	57.826001907, −152.325036589.	57.816486609, −152.325036589.
262	66.837046801, −162.617184378.	66.856648663, −162.617184378.	66.856648663, −162.565302627.	66.837046801, −162.565302627.
263	36.900584673, −76.30409839	36.903859448, −76.30409839	36.903859448, −76.300769409.	36.900584673, −76.300769409.
264	39.080371583, −94.283657449.	39.111476783, −94.283657449.	39.111476783, −94.21198472	39.080371583, −94.21198472.
265	38.0785775370001, −92.6119067879999.	38.0962204240001, −92.6119067879999.	38.0962204240001, −92.5989103479999.	38.0785775370001, −92.5989103479999.
266	29.1085864770001, −100.811107299.	29.3792559920001, −100.811107299.	29.3792559920001, −100.460775759.	29.1085864770001, −100.460775759.
267	39.979501278, −77.766381881.	40.061676766, −77.766381881.	40.061676766, −77.627738092.	39.979501278, −77.627738092.
268	40.8367062990001, −96.759207222.	40.8453505060001, −96.759207222.	40.8453505060001, −96.74825231.	40.8367062990001, −96.74825231.
269	68.865164727, −166.153805131.	68.877996761, −166.153805131.	68.877996761, −166.053355378.	68.865164727, −166.053355378.
270	34.881841514, −92.178033909.	34.928710282, −92.178033909.	34.928710282, −92.097368909.	34.881841514, −92.097368909.
271	33.7407601990001, −118.234788427.	33.7451476500001, −118.234788427.	33.7451476500001, −118.232155662.	33.7407601990001, −118.232155662.
272	32.646434739, −94.170119305.	32.694891651, −94.170119305.	32.694891651, −94.10955796	32.646434739, −94.10955796.
273	33.916514003, −118.449299679.	34.057048416, −118.449299679.	34.057048416, −118.378717014.	33.916514003, −118.378717014.
274	33.8581476250001, −118.23660337.	33.8593838490001, −118.23660337.	33.8593838490001, −118.235035273.	33.8581476250001, −118.235035273.
275	38.173833589, −85.7272245249999.	38.181490413, −85.7272245249999.	38.181490413, −85.7200947549999.	38.173833589, −85.7200947549999.
276	31.812802193, −85.654704728.	31.818371904, −85.654704728.	31.818371904, −85.646082241.	31.812802193, −85.646082241.
277	18.439120508, −65.9970120469999.	18.446769386, −65.9970120469999.	18.446769386, −65.9877331199999.	18.439120508, −65.9877331199999.
278	33.5136616820001, −112.545349748.	33.7241408570001, −112.545349748.	33.7241408570001, −112.319683167.	33.5136616820001, −112.319683167.
279	27.821277411, −82.537659279.	27.869304053, −82.537659279.	27.869304053, −82.469154309.	27.821277411, −82.469154309.
280	22.127046405, −159.731450362.	22.13630275, −159.731450362.	22.13630275, −159.71827724	22.127046405, −159.71827724.
281	21.5127546910001, −158.239749591.	21.5514708600001, −158.239749591.	21.5514708600001, −158.173991939.	21.5127546910001, −158.173991939
282	47.4870471620001, −111.21562151.	47.5233762890001, −111.21562151.	47.5233762890001, −111.152194907.	47.4870471620001, −111.152194907.
283	47.562267374, −122.556511461.	47.570404086, −122.556511461.	47.570404086, −122.531291341.	47.562267374, −122.531291341.
284	40.8062092000001, −82.5260369709999.	40.8156897690001, −82.5260369709999.	40.8156897690001, −82.5130393979999.	40.8062092000001, −82.5130393979999.
285	33.855508925, −117.319151995.	33.916474896, −117.319151995.	33.916474896, −117.239122083.	33.855508925, −117.239122083.
286	34.2011154190001, −116.717969816.	34.7339793100001, −116.717969816.	34.7339793100001, −115.720717569.	34.2011154190001, −115.720717569.
287	32.280961146, −80.76567248	32.510825803, −80.76567248	32.510825803, −80.65947492	32.280961146, −80.65947492.
288	34.6814644040001, −77.2763334639999.	35.076192102, −77.2763334639999.	35.076192102, −76.3302441729999.	34.6814644040001, −76.3302441729999.
289	32.833111095, −117.188623475.	32.920651119, −117.188623475.	32.920651119, −116.984937219.	32.833111095, −116.984937219.
290	34.558215246, −77.4842054699999.	34.746048414, −77.4842054699999.	34.746048414, −77.370277147.	34.558215246, −77.370277147.
291	32.622994906, −114.64004722.	32.679820865, −114.64004722.	32.679820865, −114.578207704.	32.622994906, −114.578207704.
292	34.4950770080001, −77.6073096539999.	34.7485511280001, −77.6073096539999.	34.7485511280001, −77.177756721.	34.4950770080001, −77.177756721.

TABLE 1 TO § 202.1401—Continued

Area ID				
293	33.205532089, −117.596249485.	33.503658101, −117.596249485.	33.503658101, −117.249972307.	33.205532089, −117.249972307.
294	21.4274913960001, −157.778625985.	21.4626192360001, −157.778625985.	21.4626192360001, −157.722086618.	21.4274913960001, −157.722086618.
295	21.38026423, −157.914545183.	21.392788317, −157.914545183.	21.392788317, −157.897882367.	21.38026423, −157.897882367.
296	38.4790113490001, −77.609862936.	38.6440896410001, −77.609862936.	38.6440896410001, −77.283059322.	38.4790113490001, −77.283059322.
297	31.5437915750001, −84.095978531.	31.5617240260001, −84.095978531.	31.5617240260001, −84.007643854.	31.5437915750001, −84.007643854.
298	34.8434594240001, −116.97121195.	34.8817582680001, −116.97121195.	34.8817582680001, −116.909128396.	34.8434594240001, −116.909128396.
299	38.5154624990001, −77.3711151099999.	38.5235364690001, −77.3711151099999.	38.5235364690001, −77.3589766939999.	38.5154624990001, −77.3589766939999.
300	30.391006078, −81.537656096.	30.413437169, −81.537656096.	30.413437169, −81.509630857.	30.391006078, −81.509630857.
301	38.828254514, −77.120041471.	38.831963061, −77.120041471.	38.831963061, −77.114666209.	38.828254514, −77.114666209.
302	39.32514001, −76.4241855929999.	39.337202481, −76.4241855929999.	39.337202481, −76.4075152099999.	39.32514001, −76.4075152099999.
303	48.1206874690001, −122.17350321.	48.1263336970001, −122.17350321.	48.1263336970001, −122.168283314.	48.1206874690001, −122.168283314.
304	32.365364879, −86.376531674.	32.415623844, −86.376531674.	32.415623844, −86.232684034.	32.365364879, −86.232684034.
305	21.3463596610001, −157.732313131.	21.3809869910001, −157.732313131.	21.3809869910001, −157.706839578.	21.3463596610001, −157.706839578.
306	34.75300134, −96.021930066	34.887500702, −96.021930066.	34.887500702, −95.825334438.	34.75300134, −95.825334438.
307	38.6375594030001, −121.429181885.	38.6902393680001, −121.429181885.	38.6902393680001, −121.382899272.	38.6375594030001, −121.382899272.
308	37.5874487990001, −97.29929204.	37.6560529930001, −97.29929204.	37.6560529930001, −97.2134855509999.	37.5874487990001, −97.2134855509999.
309	33.90292894, −80.822110255	33.94386779, −80.822110255	33.94386779, −80.780803864	33.90292894, −80.780803864.
310	35.800297926, −84.013675843.	35.822581272, −84.013675843.	35.822581272, −83.989979889.	35.800297926, −83.989979889.
311	38.36798888, −81.594851531	38.378026582, −81.594851531.	38.378026582, −81.58529054	38.36798888, −81.58529054.
312	32.7348147280001, −117.209483129.	32.7455697900001, −117.209483129.	32.7455697900001, −117.184267844.	32.7348147280001, −117.184267844.
313	34.214686409, −103.863834999.	34.383336857, −103.863834999.	34.383336857, −103.668558352.	34.214686409, −103.668558352.
314	35.021000852, −89.9701571149999.	35.030015831, −89.9701571149999.	35.030015831, −89.9638125029999.	35.021000852, −89.9638125029999.
315	35.815792593, −88.754286881.	35.946160368, −88.754286881.	35.946160368, −88.646037805.	35.815792593, −88.646037805.
316	38.015441735, −122.065438909.	38.095180461, −122.065438909.	38.095180461, −121.969625159.	38.015441735, −121.969625159.
317	33.9560292030001, −78.0749530269999.	34.2460740690001, −78.0749530269999.	34.2460740690001, −77.9056468759999.	33.9560292030001, −77.9056468759999.
318	44.8853655020001, −93.222511412.	44.8980690540001, −93.222511412.	44.8980690540001, −93.19773597.	44.8853655020001, −93.19773597.
319	48.3955222490001, −101.391958779.	48.4441800980001, −101.391958779.	48.4441800980001, −101.29967086.	48.3955222490001, −101.29967086.
320	32.792070847, −117.105638208.	32.815502529, −117.105638208.	32.815502529, −117.081336656.	32.792070847, −117.081336656.
321	32.302879454, −86.410672153.	32.306804183, −86.410672153.	32.306804183, −86.3958063469999.	32.302879454, −86.3958063469999.
322	30.935302703, −83.219069939.	31.014479318, −83.219069939.	31.014479318, −83.1288484929999.	30.935302703, −83.1288484929999.
323	43.0246506180001, −115.895653384.	43.0755981900001, −115.895653384.	43.0755981900001, −115.836219587.	43.0246506180001, −115.836219587.
324	39.041961471, −85.545884974.	39.059126926, −85.545884974.	39.059126926, −85.502112731.	39.041961471, −85.502112731.
325	32.8074254250001, −115.698918811.	32.8401116740001, −115.698918811.	32.8401116740001, −115.646437997.	32.8074254250001, −115.646437997.
326	28.5876565020001, −97.628083873.	28.6265345250001, −97.628083873.	28.6265345250001, −97.584907879.	28.5876565020001, −97.584907879.
327	71.310648094, −156.674424861.	71.344323368, −156.674424861.	71.344323368, −156.617754628.	71.310648094, −156.617754628.
328	43.8597372520001, −69.95330606.	43.9103207020001, −69.95330606.	43.9103207020001, −69.909873769.	43.8597372520001, −69.909873769.

TABLE 1 TO § 202.1401—Continued

Area ID				
329	32.743470873, −97.44549275	32.787133199, −97.44549275	32.787133199, −97.413267401.	32.743470873, −97.413267401.
330	30.1941004770001, −81.7076006299999.	30.2458023780001, −81.7076006299999.	30.2458023780001, −81.6593342339999.	30.1941004770001, −81.6593342339999.
331	40.1857296150001, −75.164926593.	40.2167846540001, −75.164926593.	40.2167846540001, −75.134209434.	40.1857296150001, −75.134209434.
332	24.5560839770001, −81.722408305.	24.5971158050001, −81.722408305.	24.5971158050001, −81.653518462.	24.5560839770001, −81.653518462.
333	27.4674233900001, −97.832157771.	27.5231989330001, −97.832157771.	27.5231989330001, −97.788047634.	27.4674233900001, −97.788047634.
334	36.255073843, −119.977147505.	36.386386503, −119.977147505.	36.386386503, −119.869576662.	36.255073843, −119.869576662.
335	30.326507308, −87.352445013.	30.375924031, −87.352445013.	30.375924031, −87.257235015.	30.326507308, −87.257235015.
336	30.683881264, −87.043781272.	30.738102029, −87.043781272.	30.738102029, −86.997376436.	30.683881264, −86.997376436.
337	36.106696485, −86.67860059	36.114637747, −86.67860059	36.114637747, −86.67190118	36.106696485, −86.67190118.
338	32.6696509240001, −117.114230685.	32.6740385570001, −117.114230685.	32.6740385570001, −117.111967973.	32.6696509240001, −117.111967973.
339	38.9746589920001, −76.4937690629999.	39.0026084470001, −76.4937690629999.	39.0026084470001, −76.4487817289999.	38.9746589920001, −76.4487817289999.
340	27.61946242, −97.4505952709999.	27.718208017, −97.4505952709999.	27.718208017, −97.2437083949999.	27.61946242, −97.2437083949999.
341	29.8014398060001, −90.0485449769999.	29.8575240390001, −90.0485449769999.	29.8575240390001, −89.9938950499999.	29.8014398060001, −89.9938950499999.
342	32.499252175, −88.6318691439999.	32.602832677, −88.6318691439999.	32.602832677, −88.5064742839999.	32.499252175, −88.5064742839999.
343	36.7852781730001, −76.063232016.	36.8386906080001, −76.063232016.	36.8386906080001, −75.99817255.	36.7852781730001, −75.99817255.
344	36.760031462, −75.9846076869999.	36.818318534, −75.9846076869999.	36.818318534, −75.9490831369999.	36.760031462, −75.9490831369999.
345	38.2488191400001, −76.46369128.	38.3093935480001, −76.46369128.	38.3093935480001, −76.373549279.	38.2488191400001, −76.373549279.
346	48.311418739, −122.708096597.	48.369700655, −122.708096597.	48.369700655, −122.617753395.	48.311418739, −122.617753395.
347	35.2654343400001, −117.8902031.	36.2318077000001, −117.8902031.	36.2318077000001, −116.9249447.	35.2654343400001, −116.9249447.
348	13.3091094070001, 144.618332428.	13.5883222610001, 144.618332428.	13.5883222610001, 144.916357575.	13.3091094070001, 144.916357575.
349	47.6909210600001, −122.628044406.	47.705184112, −122.628044406.	47.705184112, −122.613798201.	47.6909210600001, −122.613798201.
350	47.6767991730001, −122.747424327.	47.7726169310001, −122.747424327.	47.7726169310001, −122.691878973.	47.6767991730001, −122.691878973.
351	47.5449361660001, −122.671768178.	47.5653870590001, −122.671768178.	47.5653870590001, −122.623883723.	47.5449361660001, −122.623883723.
352	32.675119312, −117.256218377.	32.713082807, −117.256218377.	32.713082807, −117.234025189.	32.675119312, −117.234025189.
353	32.6582935910001, −117.135977498.	32.6884541840001, −117.135977498.	32.6884541840001, −117.112975083.	32.6582935910001, −117.112975083.
354	34.088069982, −119.160456826.	34.13946678, −119.160456826.	34.13946678, −119.064184636.	34.088069982, −119.064184636.
355	34.142955882, −119.221480878.	34.175763756, −119.221480878.	34.175763756, −119.195140105.	34.142955882, −119.195140105.
356	55.5394297110001, −131.764707731.	55.5429794870001, −131.764707731.	55.5429794870001, −131.755720856.	55.5394297110001, −131.755720856.
357	46.3564572000001, −98.3483000209999.	46.3745994580001, −98.3483000209999.	46.3745994580001, −98.3233449679999.	46.3564572000001, −98.3233449679999.
358	28.581333934, −81.200124825.	28.586585157, −81.200124825.	28.586585157, −81.194259644.	28.581333934, −81.194259644.
359	18.392254736, −67.185834374.	18.405878229, −67.185834374.	18.405878229, −67.170701901.	18.392254736, −67.170701901.
360	44.6232594310001, −67.328272859.	44.7036300010001, −67.328272859.	44.7036300010001, −67.254518602.	44.6232594310001, −67.254518602.
361	38.9186807040001, −77.070549603.	38.9241721890001, −77.070549603.	38.9241721890001, −77.063519892.	38.9186807040001, −77.063519892.
362	38.8200046750001, −77.027450812.	38.8300043240001, −77.027450812.	38.8300043240001, −77.017462058.	38.8200046750001, −77.017462058.
363	38.406152209, −77.110740786.	38.43740876, −77.110740786	38.43740876, −77.0729468369999.	38.406152209, −77.0729468369999.
364	30.33369265, −89.64817211	30.417826484, −89.64817211	30.417826484, −89.557854425.	30.33369265, −89.557854425.

TABLE 1 TO § 202.1401—Continued

Area ID				
365	38.6769074200001, −76.34415482.	38.6792870940001, −76.34415482.	38.6792870940001, −76.343227801.	38.6769074200001, −76.343227801.
366	42.3047750280001, −87.845909294.	42.3249165520001, −87.845909294.	42.3249165520001, −87.828493071.	42.3047750280001, −87.828493071.
367	41.503275973, −71.330843392.	41.554006671, −71.330843392.	41.554006671, −71.30062478	41.503275973, −71.30062478.
368	36.9170290100001, −76.335615748.	36.9640415810001, −76.335615748.	36.9640415810001, −76.2618193489999.	36.9170290100001, −76.2618193489999.
369	30.748875362, −81.576797991.	30.837030033, −81.576797991.	30.837030033, −81.479993971.	30.748875362, −81.479993971.
370	41.3859700670001, −72.09385059.	41.4104621860001, −72.09385059.	41.4104621860001, −72.07728596.	41.3859700670001, −72.07728596.
371	36.8809746540001, −76.427321462.	36.8890977200001, −76.427321462.	36.8890977200001, −76.419013745.	36.8809746540001, −76.419013745.
372	38.74493505, −86.905209651	38.919755352, −86.905209651.	38.919755352, −86.6788119869999.	38.74493505, −86.6788119869999.
373	30.158883738, −85.760741626.	30.188382598, −85.760741626.	30.188382598, −85.738993885.	30.158883738, −85.738993885.
374	40.0361710110001, −75.101397768.	40.0471374300001, −75.101397768.	40.0471374300001, −75.088731354.	40.0361710110001, −75.088731354.
375	38.871230644, −76.9994186819999.	38.876356839, −76.9994186819999.	38.876356839, −76.9912418639999.	38.871230644, −76.9912418639999.
376	38.9719405210001, −77.203514559.	38.9783021020001, −77.203514559.	38.9783021020001, −77.180406372.	38.9719405210001, −77.180406372.
377	38.3186054830001, −77.051455995.	38.3591595940001, −77.051455995.	38.3591595940001, −77.014266139.	38.3186054830001, −77.014266139.
378	38.5619658580001, −77.2103647979999.	38.6069805630001, −77.2103647979999.	38.6069805630001, −77.1602485849999.	38.5619658580001, −77.1602485849999.
379	47.9738990070001, −116.566365931.	47.9810063290001, −116.566365931.	47.9810063290001, −116.520622995.	47.9738990070001, −116.520622995.
380	40.2250093260001, −74.214186736.	40.2823128210001, −74.214186736.	40.2823128210001, −74.101728286.	40.2250093260001, −74.101728286.
381	33.9177546080001, −117.576534598.	33.9314446460001, −117.576534598.	33.9314446460001, −117.562312486.	33.9177546080001, −117.562312486.
382	37.208022726, −76.633932842.	37.273612882, −76.633932842.	37.273612882, −76.522493597.	37.208022726, −76.522493597.
383	45.6322259620001, −119.895359741.	45.8065550300001, −119.895359741.	45.8065550300001, −119.455477367.	45.6322259620001, −119.455477367.
384	32.681825013, −117.229713083.	32.715125046, −117.229713083.	32.715125046, −117.180755171.	32.681825013, −117.180755171.
385	36.842303428, −76.3151234269999.	36.849661128, −76.3151234269999.	36.849661128, −76.3024406369999.	36.842303428, −76.3024406369999.
386	35.180398117, −111.749899909.	35.195319693, −111.749899909.	35.195319693, −111.736545714.	35.180398117, −111.736545714.
387	40.6710820530001, −112.091693872.	40.6820119650001, −112.091693872.	40.6820119650001, −112.057868517.	40.6710820530001, −112.057868517.
388	37.4104380160001, −122.031548936.	37.4153630160001, −122.031548936.	37.4153630160001, −122.025261936.	37.4104380160001, −122.025261936.
389	47.966605751, −122.271045712.	47.994496312, −122.271045712.	47.994496312, −122.21398207.	47.966605751, −122.21398207.
390	30.361267243, −81.4636657189999.	30.400329774, −81.4636657189999.	30.400329774, −81.392276891.	30.361267243, −81.392276891.
391	38.976796961, −76.4937690629999.	38.986732986, −76.4937690629999.	38.986732986, −76.4761382759999.	38.976796961, −76.4761382759999.
392	38.9970659050001, −77.097142558.	39.0074154440001, −77.097142558.	39.0074154440001, −77.083297186.	38.9970659050001, −77.083297186.
393	36.9181778190001, −76.317281615.	36.933520845, −76.317281615.	36.933520845, −76.2811604669999.	36.9181778190001, −76.2811604669999.
394	40.216016376, −77.001594842.	40.239975455, −77.001594842.	40.239975455, −76.970791628.	40.216016376, −76.970791628.
395	35.3183642820001, −89.890382347.	35.3408744740001, −89.890382347.	35.3408744740001, −89.85751768.	35.3183642820001, −89.85751768.
396	36.593508146, −121.878756787.	36.600645199, −121.878756787.	36.600645199, −121.867184688.	36.593508146, −121.867184688.
397	36.8096651020001, −76.311406446.	36.8288368000001, −76.311406446.	36.8288368000001, −76.291685476.	36.8096651020001, −76.291685476.
398	32.384281554, −80.685725766.	32.394141164, −80.685725766.	32.394141164, −80.678089804.	32.384281554, −80.678089804.
399	33.729669684, −118.099622184.	33.774096004, −118.099622184.	33.774096004, −118.041605831.	33.729669684, −118.041605831.
400	36.5872707780001, −121.866360531.	36.5945029280001, −121.866360531.	36.5945029280001, −121.851862108.	36.5872707780001, −121.851862108.

TABLE 1 TO § 202.1401—Continued

Area ID				
401	36.2034528880001, −115.073249953.	36.3992515790001, −115.073249953.	36.3992515790001, −114.91920859.	36.2034528880001, −114.91920859.
402	36.4668551030001, −117.094718948.	37.9076912670001, −117.094718948.	37.9076912670001, −115.3004082.	36.4668551030001, −115.3004082.
403	42.919235051, −71.671337464.	42.952654138, −71.671337464.	42.952654138, −71.616026331.	42.919235051, −71.616026331.
404	39.6829375310001, −75.600492457.	39.6923952360001, −75.600492457.	39.6923952360001, −75.593307553.	39.6829375310001, −75.593307553.
405	43.10473267, −70.797901469	43.107704771, −70.797901469.	43.107704771, −70.7919169979999.	43.10473267, −70.7919169979999.
406	33.568962911, −86.751872966.	33.57308195, −86.751872966	33.57308195, −86.748821474	33.568962911, −86.748821474.
407	61.599438526, −149.390055835.	61.606721914, −149.390055835.	61.606721914, −149.35973238.	61.599438526, −149.35973238.
408	36.013579803, −115.202476334.	36.020786485, −115.202476334.	36.020786485, −115.198858962.	36.013579803, −115.198858962.
409	45.079114062, −93.178546539.	45.108075439, −93.178546539.	45.108075439, −93.147375066.	45.079114062, −93.147375066.
410	33.7189514350001, −84.361650185.	33.7254539750001, −84.361650185.	33.7254539750001, −84.356222295.	33.7189514350001, −84.356222295.
411	44.080835533, −70.290540358.	44.094617619, −70.290540358.	44.094617619, −70.272902712.	44.080835533, −70.272902712.
412	42.546251763, −71.589424731.	42.551133712, −71.589424731.	42.551133712, −71.5781617369999.	42.546251763, −71.5781617369999.
413	44.8040301450001, −68.8467649249999.	44.8172629220001, −68.8467649249999.	44.8172629220001, −68.8068680369999.	44.8040301450001, −68.8068680369999.
414	30.354065667, −91.146045237.	30.360422127, −91.146045237.	30.360422127, −91.1353207689999.	30.354065667, −91.1353207689999.
415	31.4025019330001, −92.335343385.	31.4795765740001, −92.335343385.	31.4795765740001, −92.245795576.	31.4025019330001, −92.245795576.
416	40.0877668460001, −83.068853255.	40.0907737950001, −83.068853255.	40.0907737950001, −83.066002311.	40.0877668460001, −83.066002311.
417	44.022196352, −121.133291583.	44.029392756, −121.133291583.	44.029392756, −121.123271772.	44.022196352, −121.123271772.
418	30.173439579, −97.674627878.	30.178958121, −97.674627878.	30.178958121, −97.668747043.	30.173439579, −97.668747043.
419	38.5445306760001, −75.0682735199999.	38.5510787900001, −75.0682735199999.	38.5510787900001, −75.0589773919999.	38.5445306760001, −75.0589773919999.
420	44.1016551610001, −121.17360693.	44.3272733540001, −121.17360693.	44.3272733540001, −121.058161787.	44.1016551610001, −121.058161787.
421	46.827120683, −100.725445186.	46.832772324, −100.725445186.	46.832772324, −100.715045706.	46.827120683, −100.715045706.
422	44.392304805, −70.947124474.	44.402273905, −70.947124474.	44.402273905, −70.928234819.	44.392304805, −70.928234819.
423	47.549068751, −122.684072241.	47.556350796, −122.684072241.	47.556350796, −122.678571789.	47.549068751, −122.678571789.
424	33.4426391850001, −112.60836981.	33.4939449270001, −112.60836981.	33.4939449270001, −112.590831261.	33.4426391850001, −112.590831261.
425	41.788965498, −80.0518139389999.	41.798009108, −80.0518139389999.	41.798009108, −80.0425795319999.	41.788965498, −80.0425795319999.
426	44.708559069, −123.281143191.	44.72023512, −123.281143191.	44.72023512, −123.259641857.	44.708559069, −123.259641857.
427	41.056686573, −96.34425821	41.096850084, −96.34425821	41.096850084, −96.326681639.	41.056686573, −96.326681639.
428	39.2163393430001, −86.1037530039999.	39.3929446850001, −86.1037530039999.	39.3929446850001, −85.9785740709999.	39.2163393430001, −85.9785740709999.
429	31.3661086110001, −92.4083963209999.	31.3916242780001, −92.4083963209999.	31.3916242780001, −92.3608840609999.	31.3661086110001, −92.3608840609999.
430	31.6146126890001, −98.960277256.	31.6667772080001, −98.960277256.	31.6667772080001, −98.901021764.	31.6146126890001, −98.901021764.
431	41.607753723, −71.505549174.	41.623638419, −71.505549174.	41.623638419, −71.491180453.	41.607753723, −71.491180453.
432	47.6525289910001, −98.9417105379999.	48.0636008830001, −98.9417105379999.	48.0636008830001, −98.6003789309999.	47.6525289910001, −98.6003789309999.
433	35.5952678190001, −95.22118754.	35.7838291280001, −95.22118754.	35.7838291280001, −95.126697455.	35.5952678190001, −95.126697455.
434	41.9394829350001, −72.670901858.	41.9441994120001, −72.670901858.	41.9441994120001, −72.661211157.	41.9394829350001, −72.661211157.
435	34.8124732220001, −92.3897548209999.	34.9614877180001, −92.3897548209999.	34.9614877180001, −92.2396274969999.	34.8124732220001, −92.2396274969999.
436	30.3094558060001, −97.768694553.	30.3273409100001, −97.768694553.	30.3273409100001, −97.756391927.	30.3094558060001, −97.756391927.

TABLE 1 TO § 202.1401—Continued

Area ID				
437	33.774194279, −95.606477742.	33.832753059, −95.606477742.	33.832753059, −95.526066382.	33.774194279, −95.526066382.
438	32.5353248810001, −93.475517374.	32.5878534930001, −93.475517374.	32.5878534930001, −93.320012082.	32.5353248810001, −93.320012082.
439	41.328015147, −72.192567648.	41.334274179, −72.192567648.	41.334274179, −72.18300523	41.328015147, −72.18300523.
440	43.2872218000001, −116.090973157.	43.3084647600001, −116.090973157.	43.3084647600001, −116.006279152.	43.2872218000001, −116.006279152.
441	41.5296110640001, −83.029247488.	41.5564763520001, −83.029247488.	41.5564763520001, −83.011583492.	41.5296110640001, −83.011583492.
442	44.0771040870001, −103.272190023.	44.0820854380001, −103.272190023.	44.0820854380001, −103.262202287.	44.0771040870001, −103.262202287.
443	41.1628317710001, −81.1929117339999.	41.2310363250001, −81.1929117339999.	41.2310363250001, −80.97584481.	41.1628317710001, −80.97584481.
444	46.07222877, −94.558733336	46.331943757, −94.558733336.	46.331943757, −94.325692646.	46.07222877, −94.325692646.
445	39.34839557, −82.9650961519999.	39.360752962, −82.9650961519999.	39.360752962, −82.9383779209999.	39.34839557, −82.9383779209999.
446	41.29766305, −73.975066263	41.324571403, −73.975066263.	41.324571403, −73.930650098.	41.29766305, −73.930650098.
447	30.2132250780001, −97.335768978.	30.310193057, −97.335768978.	30.310193057, −97.247469425.	30.2132250780001, −97.247469425.
448	30.310456754, −89.821504134.	30.336315048, −89.821504134.	30.336315048, −89.7963621059999.	30.310456754, −89.7963621059999.
449	43.922486604, −90.276809935.	43.932735952, −90.276809935.	43.932735952, −90.261339487.	43.922486604, −90.261339487.
450	45.4105970370001, −122.564234834.	45.4146313790001, −122.564234834.	45.4146313790001, −122.546020519.	45.4105970370001, −122.546020519.
451	30.192979226, −91.136406361.	30.209958464, −91.136406361.	30.209958464, −91.120742129.	30.192979226, −91.120742129.
452	33.671756665, −86.017370951.	33.757794604, −86.017370951.	33.757794604, −85.882188551.	33.671756665, −85.882188551.
453	40.2117159210001, −75.432393416.	40.2164501770001, −75.432393416.	40.2164501770001, −75.42374491.	40.2117159210001, −75.42374491.
454	33.6765084310001, −89.7534024129999.	33.7542460250001, −89.7534024129999.	33.7542460250001, −89.6202355929999.	33.6765084310001, −89.6202355929999.
455	39.378532207, −79.708317675.	39.454188743, −79.708317675.	39.454188743, −79.639802717.	39.378532207, −79.639802717.
456	42.27527302, −85.3763242809999.	42.336654723, −85.3763242809999.	42.336654723, −85.2764495459999.	42.27527302, −85.2764495459999.
457	34.222785926, −84.1147041419999.	34.225953578, −84.1147041419999.	34.225953578, −84.1115279319999.	34.222785926, −84.1115279319999.
458	46.8328736340001, −92.1598417499999.	46.8345283600001, −92.1598417499999.	46.8345283600001, −92.1578269679999.	46.8328736340001, −92.1578269679999.
459	43.14072293, −115.657766227.	43.147995984, −115.657766227.	43.147995984, −115.647820427.	43.14072293, −115.647820427.
460	38.949813614, −79.985745343.	38.958420468, −79.985745343.	38.958420468, −79.972014372.	38.949813614, −79.972014372.
461	31.3824479420001, −92.317091139.	31.4098514070001, −92.317091139.	31.4098514070001, −92.279692875.	31.3824479420001, −92.279692875.
462	44.4989956200001, −73.174626073.	44.5216654230001, −73.174626073.	44.5216654230001, −73.151341101.	44.4989956200001, −73.151341101.
463	33.05649478, −111.387806148.	33.118281303, −111.387806148.	33.118281303, −111.318954206.	33.05649478, −111.318954206.
464	36.276929619, −115.061711815.	36.307014017, −115.061711815.	36.307014017, −115.024997297.	36.276929619, −115.024997297.
465	36.9652916110001, −78.019676053.	37.1220791840001, −78.019676053.	37.1220791840001, −77.838557255.	36.9652916110001, −77.838557255.
466	35.177556168, −94.342568303.	35.36254474, −94.342568303	35.36254474, −94.026321036	35.177556168, −94.026321036.
467	40.3805917540001, −76.740923494.	40.4828843550001, −76.740923494.	40.4828843550001, −76.526125382.	40.3805917540001, −76.526125382.
468	33.7233962760001, −85.799971241.	33.7412047100001, −85.799971241.	33.7412047100001, −85.77787227.	33.7233962760001, −85.77787227.
469	32.8348369830001, −98.0657312119999.	32.8906953370001, −98.0657312119999.	32.8906953370001, −97.9964332349999.	32.8348369830001, −97.9964332349999.
470	32.775847904, −97.4626718379999.	32.781682325, −97.4626718379999.	32.781682325, −97.4528046649999.	32.775847904, −97.4528046649999.
471	38.1716157600001, −84.921448944.	38.1966283680001, −84.921448944.	38.1966283680001, −84.894209462.	38.1716157600001, −84.894209462.
472	18.002735849, −66.5139236319999.	18.025884249, −66.5139236319999.	18.025884249, −66.4942110159999.	18.002735849, −66.4942110159999.

TABLE 1 TO § 202.1401—Continued

Area ID				
473	21.2573388270001, −157.811868495.	21.2696069680001, −157.811868495.	21.2696069680001, −157.793708924.	21.2573388270001, −157.793708924.
474	33.910428789, −84.5361533929999.	33.916196229, −84.5361533929999.	33.916196229, −84.522565546.	33.910428789, −84.522565546.
475	40.959663633, −98.301445179.	40.964149849, −98.301445179.	40.964149849, −98.296290336.	40.959663633, −98.296290336.
476	40.515397589, −98.298239402.	40.567785704, −98.298239402.	40.567785704, −98.259993615.	40.515397589, −98.259993615.
477	13.471680227, 144.807392696	13.476445623, 144.807392696	13.476445623, 144.812949999	13.471680227, 144.812949999.
478	30.4045289490001, −89.065284316.	30.4205257120001, −89.065284316.	30.4205257120001, −89.059168989.	30.4045289490001, −89.059168989.
479	30.520223183, −90.417497467.	30.526889408, −90.417497467.	30.526889408, −90.406882911.	30.520223183, −90.406882911.
480	39.528072455, −76.1100913129999.	39.536739552, −76.1100913129999.	39.536739552, −76.0982416589999.	39.528072455, −76.0982416589999.
481	46.6059564510001, −111.975646726.	46.6106942060001, −111.975646726.	46.6106942060001, −111.967693583.	46.6059564510001, −111.967693583.
482	40.4376721520001, −78.4170869339999.	40.4407479890001, −78.4170869339999.	40.4407479890001, −78.4124497679999.	40.4376721520001, −78.4124497679999.
483	43.659487912, −70.674869746.	43.67992728, −70.674869746	43.67992728, −70.654823081	43.659487912, −70.654823081.
484	39.7424976190001, −86.230956444.	39.7462615480001, −86.230956444.	39.7462615480001, −86.225390797.	39.7424976190001, −86.225390797.
485	35.3048305680001, −120.756679866.	35.3717978880001, −120.756679866.	35.3717978880001, −120.664040578.	35.3048305680001, −120.664040578.
486	35.594877598, −88.916399526.	35.601416549, −88.916399526.	35.601416549, −88.909521524.	35.594877598, −88.909521524.
487	29.9497813040001, −90.0120117979999.	29.9740232620001, −90.0120117979999.	29.9740232620001, −89.9987827089999.	29.9497813040001, −89.9987827089999.
488	38.8833909860001, −81.8464996549999.	38.905765642, −81.8464996549999.	38.905765642, −81.8170444439999.	38.8833909860001, −81.8170444439999.
489	39.01630591, −95.6872730109999.	39.022374526, −95.6872730109999.	39.022374526, −95.6797306829999.	39.01630591, −95.6797306829999.
490	36.4178126140001, −82.493381518.	36.4246402130001, −82.493381518.	36.4246402130001, −82.484291574.	36.4178126140001, −82.484291574.
491	21.3142785630001, −158.069986235.	21.3240454770001, −158.069986235.	21.3240454770001, −158.056465611.	21.3142785630001, −158.056465611.
492	39.764279425, −85.527190456.	39.778947386, −85.527190456.	39.778947386, −85.508361982.	39.764279425, −85.508361982.
493	44.0647301270001, −122.982252253.	44.0670417360001, −122.982252253.	44.0670417360001, −122.973786312.	44.0647301270001, −122.973786312.
494	42.766389845, −84.576207556.	42.769800145, −84.576207556.	42.769800145, −84.567413358.	42.766389845, −84.567413358.
495	32.270748628, −106.939138534.	32.280280019, −106.939138534.	32.280280019, −106.930519974.	32.270748628, −106.930519974.
496	40.2658142980001, −74.748095306.	40.2734112650001, −74.748095306.	40.2734112650001, −74.740257715.	40.2658142980001, −74.740257715.
497	35.0150424290001, −97.239011654.	35.0295356340001, −97.239011654.	35.0295356340001, −97.223711786.	35.0150424290001, −97.223711786.
498	40.8356006820001, −96.758767006.	40.8404020610001, −96.758767006.	40.8404020610001, −96.749174181.	40.8356006820001, −96.749174181.
499	33.7812372280001, −118.067627933.	33.8016134000001, −118.067627933.	33.8016134000001, −118.032767969.	33.7812372280001, −118.032767969.
500	32.8597198360001, −83.6073436619999.	32.8630748340001, −83.6073436619999.	32.8630748340001, −83.6039690959999.	32.8597198360001, −83.6039690959999.
501	39.636663701, −92.534704178.	39.721017576, −92.534704178.	39.721017576, −92.464676968.	39.636663701, −92.464676968.
502	41.267041534, −88.7046910729999.	41.305913573, −88.7046910729999.	41.305913573, −88.6608137729999.	41.267041534, −88.6608137729999.
503	29.426494618, −98.3843199139999.	29.437625079, −98.3843199139999.	29.437625079, −98.3746227379999.	29.426494618, −98.3746227379999.
504	39.6487077620001, −81.847046613.	39.6734994180001, −81.847046613.	39.6734994180001, −81.831592537.	39.6487077620001, −81.831592537.
505	44.9048285740001, −123.003047071.	44.9170262920001, −123.003047071.	44.9170262920001, −122.995194144.	44.9048285740001, −122.995194144.
506	41.1829986970001, −96.49160163.	41.2049128990001, −96.49160163.	41.2049128990001, −96.425755553.	41.1829986970001, −96.425755553.
507	43.7601885300001, −98.047917175.	43.7638707560001, −98.047917175.	43.7638707560001, −98.039102093.	43.7601885300001, −98.039102093.
508	32.4031817050001, −86.263631114.	32.4082452810001, −86.263631114.	32.4082452810001, −86.2557011.	32.4031817050001, −86.2557011.

TABLE 1 TO § 202.1401—Continued

Area ID				
509	36.1649285010001, −78.833628877.	36.2232305700001, −78.833628877.	36.2232305700001, −78.75963967.	36.1649285010001, −78.75963967.
510	37.81235573, −94.3097107569999.	37.828354979, −94.3097107569999.	37.828354979, −94.2731087829999.	37.81235573, −94.2731087829999.
511	36.7579974450001, −94.387727354.	36.8328900980001, −94.387727354.	36.8328900980001, −94.326852463.	36.7579974450001, −94.326852463.
512	42.5267790020001, −71.08203514.	42.5603767370001, −71.08203514.	42.5603767370001, −71.063291358.	42.5267790020001, −71.063291358.
513	39.4912259380001, −76.8607346809999.	39.5046787930001, −76.8607346809999.	39.5046787930001, −76.8318924949999.	39.4912259380001, −76.8318924949999.
514	46.1080148720001, −123.964495138.	46.1501140200001, −123.964495138.	46.1501140200001, −123.92502133.	46.1080148720001, −123.92502133.
515	17.9872158480001, −66.333706182.	18.0695436220001, −66.333706182.	18.0695436220001, −66.240579825.	17.9872158480001, −66.240579825.
516	33.780577163, −82.2952040439999.	33.807394959, −82.2952040439999.	33.807394959, −82.26292394	33.780577163, −82.26292394.
517	46.6005921770001, −112.190250013.	46.6592451280001, −112.190250013.	46.6592451280001, −112.094472322.	46.6005921770001, −112.094472322.
518	39.423596381, −76.51081268	39.439023401, −76.51081268	39.439023401, −76.496156333.	39.423596381, −76.496156333.
519	46.220510372, −111.635118944.	46.337394743, −111.635118944.	46.337394743, −111.504109039.	46.220510372, −111.504109039.
520	42.1437413450001, −104.948278987.	42.4788211760001, −104.948278987.	42.4788211760001, −104.703889369.	42.1437413450001, −104.703889369.
521	35.656031539, −95.375341077.	35.664828514, −95.375341077.	35.664828514, −95.369972431.	35.656031539, −95.369972431.
522	36.0958233040001, −86.7615681459999.	36.1023428190001, −86.7615681459999.	36.1023428190001, −86.7562354.	36.0958233040001, −86.7562354.
523	40.9786701780001, −80.325759923.	40.9800945050001, −80.325759923.	40.9800945050001, −80.323839076.	40.9786701780001, −80.323839076.
524	35.2622862810001, −97.4851407689999.	35.2681205800001, −97.4851407689999.	35.2681205800001, −97.4768490759999.	35.2622862810001, −97.4768490759999.
525	33.6157453390001, −84.3128273029999.	33.6193347170001, −84.3128273029999.	33.6193347170001, −84.3074772369999.	33.6157453390001, −84.3074772369999.
526	33.4618850200001, −111.969623276.	33.4727567890001, −111.969623276.	33.4727567890001, −111.952212294.	33.4618850200001, −111.952212294.
527	32.6578846960001, −111.495190228.	32.6688813430001, −111.495190228.	32.6688813430001, −111.481955968.	32.6578846960001, −111.481955968.
528	35.804791455, −78.715406802.	35.81355058, −78.715406802	35.81355058, −78.707216709	35.804791455, −78.707216709.
529	39.8002476090001, −82.9570252779999.	39.8098625370001, −82.9570252779999.	39.8098625370001, −82.94567622.	39.8002476090001, −82.94567622.
530	35.3683435470001, −106.65493619.	35.3777845520001, −106.65493619.	35.3777845520001, −106.648878128.	35.3683435470001, −106.648878128.
531	39.627394171, −75.6147487649999.	39.639382105, −75.6147487649999.	39.639382105, −75.6006753489999.	39.627394171, −75.6006753489999.
532	43.9963073710001, −92.433533997.	43.9977499120001, −92.433533997.	43.9977499120001, −92.428949024.	43.9963073710001, −92.428949024.
533	44.7463851480001, −93.12881708.	44.7488195410001, −93.12881708.	44.7488195410001, −93.125978095.	44.7463851480001, −93.125978095.
534	32.284284584, −86.3990584479999.	32.295043619, −86.3990584479999.	32.295043619, −86.392323549.	32.284284584, −86.392323549.
535	32.847954014, −97.3530685539999.	32.861579522, −97.3530685539999.	32.861579522, −97.3432426939999.	32.847954014, −97.3432426939999.
536	37.030464438, −113.549169301.	37.037578732, −113.549169301.	37.037578732, −113.544639	37.030464438, −113.544639.
537	38.7817203050001, −97.642976177.	38.7897490390001, −97.642976177.	38.7897490390001, −97.633242512.	38.7817203050001, −97.633242512.
538	37.49085725, −77.3171608389999.	37.498350787, −77.3171608389999.	37.498350787, −77.3077128829999.	37.49085725, −77.3077128829999.
539	35.5622835610001, −106.10286838.	35.5754168170001, −106.10286838.	35.5754168170001, −106.071788538.	35.5622835610001, −106.071788538.
540	40.1177429000001, −74.044914025.	40.1299027480001, −74.044914025.	40.1299027480001, −74.030081087.	40.1177429000001, −74.030081087.
541	39.576923987, −85.816200007.	39.580378098, −85.816200007.	39.580378098, −85.807738311.	39.576923987, −85.807738311.
542	32.519546491, −111.340100133.	32.527987523, −111.340100133.	32.527987523, −111.325196238.	32.519546491, −111.325196238.
543	43.5730602740001, −96.6930749859999.	43.5983048400001, −96.6930749859999.	43.5983048400001, −96.6759672029999.	43.5730602740001, −96.6759672029999.
544	25.9569713660001, −80.31070355.	25.9681289730001, −80.31070355.	25.9681289730001, −80.298558922.	25.9569713660001, −80.298558922.

TABLE 1 TO § 202.1401—Continued

Area ID				
545	38.131120233, −89.745599204.	38.190313565, −89.745599204.	38.190313565, −89.703313722.	38.131120233, −89.703313722.
546	40.1880831510001, −75.561069736.	40.1918052850001, −75.561069736.	40.1918052850001, −75.552580986.	40.1880831510001, −75.552580986.
547	39.8160693520001, −89.673473292.	39.8306927080001, −89.673473292.	39.8306927080001, −89.664369884.	39.8160693520001, −89.664369884.
548	37.2490490960001, −93.395772062.	37.2571610570001, −93.395772062.	37.2571610570001, −93.384982394.	37.2490490960001, −93.384982394.
549	45.5372774640001, −94.060060866.	45.5419761270001, −94.060060866.	45.5419761270001, −94.051145099.	45.5372774640001, −94.051145099.
550	45.5645070200001, −94.179496597.	45.5652420030001, −94.179496597.	45.5652420030001, −94.175345802.	45.5645070200001, −94.175345802.
551	36.8110053980001, −75.9894743689999.	36.8227442360001, −75.9894743689999.	36.8227442360001, −75.9659250589999.	36.8110053980001, −75.9659250589999.
552	41.3451753470001, −72.293373883.	41.3813569730001, −72.293373883.	41.3813569730001, −72.253317667.	41.3451753470001, −72.253317667.
553	36.285694226, −95.309758124.	36.300130892, −95.309758124.	36.300130892, −95.278470963.	36.285694226, −95.278470963.
554	43.2708696780001, −71.1288204539999.	43.2848092560001, −71.1288204539999.	43.2848092560001, −71.1155219099999.	43.2708696780001, −71.1155219099999.
555	44.4965394450001, −73.168838485.	44.5034995140001, −73.168838485.	44.5034995140001, −73.160140825.	44.4965394450001, −73.160140825.
556	44.442952367, −72.960320316.	44.500157333, −72.960320316.	44.500157333, −72.836710736.	44.442952367, −72.836710736.
557	38.546453582, −92.080098162.	38.556080633, −92.080098162.	38.556080633, −92.055385571.	38.546453582, −92.055385571.
558	19.696784098, −155.052848025.	19.715068265, −155.052848025.	19.715068265, −155.023635733.	19.696784098, −155.023635733.
559	36.8796769900001, −90.310798339.	36.9046015270001, −90.310798339.	36.9046015270001, −90.255783907.	36.8796769900001, −90.255783907.
560	39.441791832, −79.6837218599999.	39.464465755, −79.6837218599999.	39.464465755, −79.6475069149999.	39.441791832, −79.6475069149999.
561	34.9067538520001, −85.070727678.	34.9506642170001, −85.070727678.	34.9506642170001, −85.045031881.	34.9067538520001, −85.045031881.
562	35.814732012, −88.7542933719999.	35.923989023, −88.7542933719999.	35.923989023, −88.6437411839999.	35.814732012, −88.6437411839999.
563	36.006276454, −86.516501852.	36.027518046, −86.516501852.	36.027518046, −86.492335009.	36.006276454, −86.492335009.
564	44.067527784, −103.325214534.	44.0784787400001, −103.325214534.	44.0784787400001, −103.287313773.	44.067527784, −103.287313773.
565	43.0833898060001, −72.4562338169999.	43.0889316040001, −72.4562338169999.	43.0889316040001, −72.4474520169999.	43.0833898060001, −72.4474520169999.
566	37.2459669690001, −87.264708566.	37.3155568590001, −87.264708566.	37.3155568590001, −87.143105234.	37.2459669690001, −87.143105234.
567	39.3487643610001, −81.448406511.	39.3590411380001, −81.448406511.	39.3590411380001, −81.437125672.	39.3487643610001, −81.437125672.
568	43.230983715, −78.987693814.	43.244098627, −78.987693814.	43.244098627, −78.957641634.	43.230983715, −78.957641634.
569	38.414110285, −90.4008158519999.	38.51933631, −90.4008158519999.	38.51933631, −89.8873624389999.	38.414110285, −89.8873624389999.
570	43.1058774480001, −78.9722862359999.	43.1213964380001, −78.9722862359999.	43.1213964380001, −78.9269798539999.	43.1058774480001, −78.9269798539999.
571	38.8465829040001, −76.9406129989999.	38.8511023340001, −76.9406129989999.	38.8511023340001, −76.9338436309999.	38.8465829040001, −76.9338436309999.
572	36.799812242, −76.299262352.	36.806581273, −76.299262352.	36.806581273, −76.291663588.	36.799812242, −76.291663588.
573	36.824516203, −76.2911109619999.	36.82654125, −76.2911109619999.	36.82654125, −76.2870895149999.	36.824516203, −76.2870895149999.
574	31.0389879680001, −87.076766692.	31.0572498550001, −87.076766692.	31.0572498550001, −87.053283792.	31.0389879680001, −87.053283792.
575	30.486569113, −86.966743959.	30.523283452, −86.966743959.	30.523283452, −86.940434633.	30.486569113, −86.940434633.
576	31.4033835660001, −87.057347927.	31.4251772980001, −87.057347927.	31.4251772980001, −87.022039826.	31.4033835660001, −87.022039826.
577	30.417555556, −86.9026103099999.	30.432862018, −86.9026103099999.	30.432862018, −86.8837180249999.	30.417555556, −86.8837180249999.
578	30.599791442, −86.950876547.	30.619098213, −86.950876547.	30.619098213, −86.9265002429999.	30.599791442, −86.9265002429999.
579	30.5546267450001, −87.8164634139999.	30.5687059560001, −87.8164634139999.	30.5687059560001, −87.8015463849999.	30.5546267450001, −87.8015463849999.
580	30.617963515, −87.148395847.	30.632703528, −87.148395847.	30.632703528, −87.131141293.	30.617963515, −87.131141293.

TABLE 1 TO § 202.1401—Continued

Area ID				
581	30.499075884, −87.6626447849999.	30.520323757, −87.6626447849999.	30.520323757, −87.6311911829999.	30.499075884, −87.6311911829999.
582	30.338386572, −87.5495986079999.	30.351971261, −87.5495986079999.	30.351971261, −87.5332728869999.	30.338386572, −87.5332728869999.
583	35.3381397860001, −89.875828209.	35.3503400000001, −89.875828209.	35.3503400000001, −89.848676466.	35.3381397860001, −89.848676466.
584	36.535830635, −76.292027831.	36.580439287, −76.292027831.	36.580439287, −76.243039727.	36.535830635, −76.243039727.
585	33.891359251, −118.072946629.	33.894991619, −118.072946629.	33.894991619, −118.067394654.	33.891359251, −118.067394654.
586	38.3285014350001, −76.4841629759999.	38.3442330700001, −76.4841629759999.	38.3442330700001, −76.4639193759999.	38.3285014350001, −76.4639193759999.
587	43.077684909, −73.823802707.	43.082196982, −73.823802707.	43.082196982, −73.818216923.	43.077684909, −73.818216923.
588	18.4266523270001, −66.188700669.	18.4276186450001, −66.188700669.	18.4276186450001, −66.187788338.	18.4266523270001, −66.187788338.
589	35.086256399, −90.1438097929999.	35.090263498, −90.1438097929999.	35.090263498, −90.138466962.	35.086256399, −90.138466962.
590	42.4740966470001, −71.292022302.	42.4801271500001, −71.292022302.	42.4801271500001, −71.286586841.	42.4740966470001, −71.286586841.
591	41.0982621430001, −95.9280611469999.	41.1364452900001, −95.9280611469999.	41.1364452900001, −95.8780365989999.	41.0982621430001, −95.8780365989999.
592	32.7452306660001, −117.200217282.	32.7528565660001, −117.200217282.	32.7528565660001, −117.192605845.	32.7452306660001, −117.192605845.
593	32.783231948, −88.8532491779999.	32.814254912, −88.8532491779999.	32.814254912, −88.8124127399999.	32.783231948, −88.8124127399999.
594	30.37231968, −87.429057305	30.394059181, −87.429057305.	30.394059181, −87.396697185.	30.37231968, −87.396697185.
595	48.1708872200001, −122.648186576.	48.2120255960001, −122.648186576.	48.2120255960001, −122.615173447.	48.1708872200001, −122.615173447.
596	30.338350216, −81.889129182.	30.377897748, −81.889129182.	30.377897748, −81.84492402	30.338350216, −81.84492402.
597	70.488162834, −149.926235024.	70.509905742, −149.926235024.	70.509905742, −149.855544128.	70.488162834, −149.855544128.
598	43.098523582, −116.31428757.	43.37173967, −116.31428757	43.37173967, −115.957075202.	43.098523582, −115.957075202.
599	38.0231563570001, −122.170412652.	38.0284346090001, −122.170412652.	38.0284346090001, −122.162692799.	38.0231563570001, −122.162692799.
600	21.979075729, −159.787895529.	22.073530219, −159.787895529.	22.073530219, −159.750843749.	21.979075729, −159.750843749.
601	37.709457716, −121.91515472.	37.747451286, −121.91515472.	37.747451286, −121.871676143.	37.709457716, −121.871676143.
602	28.2124892410001, −80.6189925959999.	28.2719774110001, −80.6189925959999.	28.2719774110001, −80.5967212699999.	28.2124892410001, −80.5967212699999.
603	21.3812730710001, −157.972837384.	21.3857579590001, −157.972837384.	21.3857579590001, −157.969830103.	21.3812730710001, −157.969830103.
604	43.0830098340001, −70.8265315799999.	43.095680228, −70.8265315799999.	43.095680228, −70.8118178159999.	43.0830098340001, −70.8118178159999.
605	38.8665872170001, −77.06187689.	38.8804333410001, −77.06187689.	38.8804333410001, −77.0457741439999.	38.8665872170001, −77.0457741439999.
606	38.805877954, −104.720171001.	38.838836254, −104.720171001.	38.838836254, −104.673427575.	38.805877954, −104.673427575.
607	40.9140682660001, −74.590780383.	40.9956152640001, −74.590780383.	40.9956152640001, −74.494014259.	40.9140682660001, −74.494014259.
608	18.26752057, −65.759072139	18.26922761, −65.759072139	18.26922761, −65.757502273	18.26752057, −65.757502273.
609	37.495160689, −122.500638613.	37.504255663, −122.500638613.	37.504255663, −122.494186302.	37.495160689, −122.494186302.
610	34.2702027120001, −92.13996888.	34.3785932240001, −92.13996888.	34.3785932240001, −92.033468658.	34.2702027120001, −92.033468658.
611	18.2467234310001, −65.600381523.	18.2570859030001, −65.600381523.	18.2570859030001, −65.5822592889999.	18.2467234310001, −65.5822592889999.
612	37.339590329, −104.173059108.	37.644554428, −104.173059108.	37.644554428, −103.576450075.	37.339590329, −103.576450075.
613	40.489967456, −80.215160815.	40.497923194, −80.215160815.	40.497923194, −80.205677052.	40.489967456, −80.205677052.
614	40.4899753650001, −80.215361211.	40.4979311050001, −80.215361211.	40.4979311050001, −80.205680084.	40.4899753650001, −80.205680084.
615	19.580002141, −155.753584385.	19.935340889, −155.753584385.	19.935340889, −155.482149063.	19.580002141, −155.482149063.
616	33.737668318, −80.5168304859999.	33.849728431, −80.5168304859999.	33.849728431, −80.4450008049999.	33.737668318, −80.4450008049999.

TABLE 1 TO § 202.1401—Continued

Area ID				
617	38.887515787, −123.552272552.	38.895551718, −123.552272552.	38.895551718, −123.538718114.	38.887515787, −123.538718114.
618	71.323665191, −156.649567453.	71.336534761, −156.649567453.	71.336534761, −156.601540334.	71.323665191, −156.601540334.
619	45.57436111, −122.604832246.	45.583315392, −122.604832246.	45.583315392, −122.585382407.	45.57436111, −122.585382407.
620	42.9087822710001, −71.4221747879999.	43.0870732990001, −71.4221747879999.	43.0870732990001, −70.722436956.	42.9087822710001, −70.722436956.
621	36.594597106, −121.926941695.	36.608467628, −121.926941695.	36.608467628, −121.894607972.	36.594597106, −121.894607972.
622	38.263930139, −104.386297178.	38.360999196, −104.386297178.	38.360999196, −104.275724057.	38.263930139, −104.275724057.
623	38.290060253, −77.0671300829999.	38.31683736, −77.0671300829999.	38.31683736, −77.0170631189999.	38.290060253, −77.0170631189999.
624	21.3139823400001, −157.992793478.	21.3226045200001, −157.992793478.	21.3226045200001, −157.982066252.	21.3139823400001, −157.982066252.
625	41.5907533440001, −71.42348666.	41.6007626130001, −71.42348666.	41.6007626130001, −71.41187911.	41.5907533440001, −71.41187911.
626	37.163382287, −80.5791188709999.	37.207412609, −80.5791188709999.	37.207412609, −80.5101282629999.	37.163382287, −80.5101282629999.
627	18.5087916470001, −67.099861576.	18.5101598370001, −67.099861576.	18.5101598370001, −67.098621282.	18.5087916470001, −67.098621282.
628	33.397278645, −94.4116859869999.	33.464838472, −94.4116859869999.	33.464838472, −94.3047919909999.	33.397278645, −94.3047919909999.
629	44.9551877580001, −70.513638005.	45.0169721250001, −70.513638005.	45.0169721250001, −70.379987151.	44.9551877580001, −70.379987151.
630	34.550284843, −86.7237782349999.	34.710900354, −86.7237782349999.	34.710900354, −86.5815630549999.	34.550284843, −86.5815630549999.
631	39.4978523080001, −119.778804811.	39.5024544730001, −119.778804811.	39.5024544730001, −119.771926612.	39.4978523080001, −119.771926612.
632	39.806889794, −82.949783742.	39.819444408, −82.949783742.	39.819444408, −82.937417355.	39.806889794, −82.937417355.
633	38.1508457090001, −78.418005901.	38.1586875990001, −78.418005901.	38.1586875990001, −78.409329548.	38.1508457090001, −78.409329548.
634	37.7110124880001, −120.921809782.	37.7227924600001, −120.921809782.	37.7227924600001, −120.9168393.	37.7110124880001, −120.9168393.
635	32.5734846130001, −83.613041736.	32.6644753900001, −83.613041736.	32.6644753900001, −83.555394419.	32.5734846130001, −83.555394419.
636	41.5101975790001, −90.566624136.	41.5236820390001, −90.566624136.	41.5236820390001, −90.515679261.	41.5101975790001, −90.515679261.
637	39.816797712, −104.880637268.	39.895272909, −104.880637268.	39.895272909, −104.796958344.	39.816797712, −104.796958344.
638	61.756264087, −166.062507434.	61.799913075, −166.062507434.	61.799913075, −165.913701567.	61.756264087, −165.913701567.
639	43.2183336890001, −75.415282906.	43.2263537340001, −75.415282906.	43.2263537340001, −75.407014028.	43.2183336890001, −75.407014028.
640	39.762626991, −94.904952104.	39.769793541, −94.904952104.	39.769793541, −94.897835881.	39.762626991, −94.897835881.
641	31.3342942350001, −86.0977289259999.	31.3453725330001, −86.0977289259999.	31.3453725330001, −86.085558079.	31.3342942350001, −86.085558079.
642	40.7838318330001, −111.959489583.	40.7949147800001, −111.959489583.	40.7949147800001, −111.953751907.	40.7838318330001, −111.953751907.
643	32.8003673640001, −118.606292107.	33.0377362220001, −118.606292107.	33.0377362220001, −118.348994062.	32.8003673640001, −118.348994062.
644	33.2121599560001, −119.582134532.	33.29062044, −119.582134532.	33.29062044, −119.418213784.	33.2121599560001, −119.418213784.
645	33.7662733170001, −118.309268541.	33.7813000720001, −118.309268541.	33.7813000720001, −118.293960351.	33.7662733170001, −118.293960351.
646	33.991029047, −119.635878529.	33.997444378, −119.635878529.	33.997444378, −119.625797527.	33.991029047, −119.625797527.
647	30.458179069, −87.351595059.	30.481667064, −87.351595059.	30.481667064, −87.33104122	30.458179069, −87.33104122.
648	42.1757726720001, −90.4077834729999.	42.284196191, −90.4077834729999.	42.284196191, −90.2282601739999.	42.1757726720001, −90.2282601739999.
649	32.119801635, −81.1976294959999.	32.13505162, −81.1976294959999.	32.13505162, −81.1837630719999.	32.119801635, −81.1837630719999.
650	42.5925001000001, −115.678838723.	42.8511848830001, −115.678838723.	42.8511848830001, −115.453730372.	42.5925001000001, −115.453730372.
651	42.8436851000001, −73.932567765.	42.8583933770001, −73.932567765.	42.8583933770001, −73.917508999.	42.8436851000001, −73.917508999.
652	38.7843530810001, −104.551986183.	38.8241032480001, −104.551986183.	38.8241032480001, −104.48867271.	38.7843530810001, −104.48867271.

TABLE 1 TO § 202.1401—Continued

Area ID				
653	38.524439918, −89.882877352.	38.558372905, −89.882877352.	38.558372905, −89.822791153.	38.524439918, −89.822791153.
654	41.402655098, −75.6679100109999.	41.405858099, −75.6679100109999.	41.405858099, −75.6641420559999.	41.402655098, −75.6641420559999.
655	36.9172616480001, −76.320386974.	36.9234795100001, −76.320386974.	36.9234795100001, −76.310890414.	36.9172616480001, −76.310890414.
656	48.26740571, −122.645903557.	48.3084303770001, −122.645903557.	48.3084303770001, −122.555529232.	48.26740571, −122.555529232.
657	42.5944000000001, −82.8511999999999.	42.6303400000001, −82.8511999999999.	42.6303400000001, −82.8038799999999.	42.5944000000001, −82.8038799999999.
658	36.237894413, −119.894821285.	36.250497998, −119.894821285.	36.250497998, −119.869682611.	36.237894413, −119.869682611.
659	60.1318770720001, −149.434449035.	60.1347511870001, −149.434449035.	60.1347511870001, −149.431802327.	60.1318770720001, −149.431802327.
660	35.3214638170001, −77.997073351.	35.368940398, −77.997073351.	35.368940398, −77.930639313.	35.3214638170001, −77.930639313.
661	33.9530524190001, −80.494323712.	33.9954038330001, −80.494323712.	33.9954038330001, −80.441564645.	33.9530524190001, −80.441564645.
662	31.3582318730001, −85.856088056.	31.3677829840001, −85.856088056.	31.3677829840001, −85.84143832.	31.3582318730001, −85.84143832.
663	33.956330827, −98.528137592.	34.017271784, −98.528137592.	34.017271784, −98.4775551939999.	33.956330827, −98.4775551939999.
664	40.1402214060001, −120.185906595.	40.2702161240001, −120.185906595.	40.2702161240001, −120.074522544.	40.1402214060001, −120.074522544.
665	32.585610327, −117.134530157.	32.609517949, −117.134530157.	32.609517949, −117.121573696.	32.585610327, −117.121573696.
666	42.3865801530001, −96.377733927.	42.3986855140001, −96.377733927.	42.3986855140001, −96.3700527519999.	42.3865801530001, −96.3700527519999.
667	31.2790279390001, −86.135253897.	31.2921867390001, −86.135253897.	31.2921867390001, −86.12630462.	31.2790279390001, −86.12630462.
668	38.5971126590001, −97.891769008.	38.7549420740001, −97.891769008.	38.7549420740001, −97.731700038.	38.5971126590001, −97.731700038.
669	32.665275626, −117.245056924.	32.670651139, −117.245056924.	32.670651139, −117.237168313.	32.665275626, −117.237168313.
670	61.088401402, −155.608677328.	61.118439774, −155.608677328.	61.118439774, −155.558809541.	61.088401402, −155.558809541.
671	39.8435710260001, −83.84415892.	39.8525313250001, −83.84415892.	39.8525313250001, −83.827046603.	39.8435710260001, −83.827046603.
672	36.7792288150001, −76.316870104.	36.7960357240001, −76.316870104.	36.7960357240001, −76.304641406.	36.7792288150001, −76.304641406.
673	38.5886024650001, −90.211334345.	38.5936509870001, −90.211334345.	38.5936509870001, −90.205345975.	38.5886024650001, −90.205345975.
674	41.491597375, −74.096301663.	41.493603532, −74.096301663.	41.493603532, −74.09231513	41.491597375, −74.09231513.
675	41.4957478590001, −74.093456875.	41.5071142860001, −74.093456875.	41.5071142860001, −74.076705335.	41.4957478590001, −74.076705335.
676	31.3556919110001, −86.019020089.	31.3632965050001, −86.019020089.	31.3632965050001, −86.009368893.	31.3556919110001, −86.009368893.
677	38.5366165980001, −77.2462204349999.	38.5562248710001, −77.2462204349999.	38.5562248710001, −77.1968327609999.	38.5366165980001, −77.1968327609999.
678	43.093425804, −76.13209217	43.105369507, −76.13209217	43.105369507, −76.117106326.	43.093425804, −76.117106326.
679	31.1194852620001, −85.983038227.	31.1263987840001, −85.983038227.	31.1263987840001, −85.975130114.	31.1194852620001, −85.975130114.
680	32.90171336, −115.830667748.	33.00155658, −115.830667748.	33.00155658, −115.679781585.	32.90171336, −115.679781585.
681	62.864848431, −156.051764799.	62.942582989, −156.051764799.	62.942582989, −155.664968137.	62.864848431, −155.664968137.
682	32.418304849, −113.683744005.	32.912746437, −113.683744005.	32.912746437, −112.306115231.	32.418304849, −112.306115231.
683	38.9884924360001, −105.010363219.	39.0140804660001, −105.010363219.	39.0140804660001, −104.991241919.	38.9884924360001, −104.991241919.
684	65.5522801760001, −168.013053723.	65.5830229910001, −168.013053723.	65.5830229910001, −167.912258962.	65.5522801760001, −167.912258962.
685	35.384500001, −97.4236999999999.	35.4497, −97.4236999999999	35.4497, −97.3502865429999	35.384500001, −97.3502865429999.
686	41.1825353090001, −75.443820828.	41.2131432310001, −75.443820828.	41.2131432310001, −75.411887882.	41.1825353090001, −75.411887882.
687	41.58166204, −83.799456627	41.59389898, −83.799456627	41.59389898, −83.786432604	41.58166204, −83.786432604.
688	40.2607276530001, −112.497273742.	40.5755204400001, −112.497273742.	40.5755204400001, −112.279088302.	40.2607276530001, −112.279088302.

TABLE 1 TO § 202.1401—Continued

Area ID				
689	31.2251159510001, −85.564347313.	31.2323695170001, −85.564347313.	31.2323695170001, −85.553616915.	31.2251159510001, −85.553616915.
690	31.3753255780001, −81.894810498.	31.6654206230001, −81.894810498.	31.6654206230001, −81.52596687.	31.3753255780001, −81.52596687.
691	38.231289094, −121.98346892.	38.294736015, −121.98346892.	38.294736015, −121.881230384.	38.231289094, −121.881230384.
692	38.3228969080001, −121.933846122.	38.3283655290001, −121.933846122.	38.3283655290001, −121.915378048.	38.3228969080001, −121.915378048.
693	21.351128573, −157.898178476.	21.367812054, −157.898178476.	21.367812054, −157.879404163.	21.351128573, −157.879404163.
694	21.4642480200001, −158.148373992.	21.5218182430001, −158.148373992.	21.5218182430001, −157.901772211.	21.4642480200001, −157.901772211.
695	43.1244504040001, −89.341539911.	43.1368306370001, −89.341539911.	43.1368306370001, −89.328466326.	43.1244504040001, −89.328466326.
696	24.5433363610001, −81.811655077.	24.5555222860001, −81.811655077.	24.5555222860001, −81.797521593.	24.5433363610001, −81.797521593.
697	24.5614307340001, −81.798222455.	24.5672092190001, −81.798222455.	24.5672092190001, −81.782640081.	24.5614307340001, −81.782640081.
698	32.127406367, −110.955077243.	32.133937736, −110.955077243.	32.133937736, −110.945092818.	32.127406367, −110.945092818.
699	36.2121647440001, −95.878742446.	36.2203832320001, −95.878742446.	36.2203832320001, −95.868966625.	36.2121647440001, −95.868966625.
700	45.07910944, −93.181911062	45.104247148, −93.181911062.	45.104247148, −93.166136656.	45.07910944, −93.166136656.
701	29.953597589, −85.6870879419999.	30.141953697, −85.6870879419999.	30.141953697, −85.444996611.	29.953597589, −85.444996611.
702	38.983678555, −76.5010465079999.	38.992477092, −76.5010465079999.	38.992477092, −76.4868322629999.	38.983678555, −76.4868322629999.
703	21.469739594, −158.057058607.	21.479496623, −158.057058607.	21.479496623, −158.050204602.	21.469739594, −158.050204602.
704	38.750330283, −104.304283339.	38.795708158, −104.304283339.	38.795708158, −104.298582551.	38.750330283, −104.298582551.
705	38.9545078850001, −104.910763947.	39.0421097770001, −104.910763947.	39.0421097770001, −104.830835276.	38.9545078850001, −104.830835276.
706	33.2114718620001, −117.39895734.	33.2146081990001, −117.39895734.	33.2146081990001, −117.395706525.	33.2114718620001, −117.395706525.
707	40.339366355, −114.13239866.	41.187663286, −114.13239866.	41.187663286, −112.775026182.	40.339366355, −112.775026182.
708	36.3075026230001, −97.932652751.	36.3645349300001, −97.932652751.	36.3645349300001, −97.890961956.	36.3075026230001, −97.890961956.
709	34.5107894400001, −120.645844615.	34.9069803380001, −120.645844615.	34.9069803380001, −120.439765984.	34.5107894400001, −120.439765984.
710	43.125429819, −75.5932489149999.	43.128384246, −75.5932489149999.	43.128384246, −75.5892130629999.	43.125429819, −75.5892130629999.
711	18.093746783, −65.5171222009999.	18.099320238, −65.5171222009999.	18.099320238, −65.5081834699999.	18.093746783, −65.5081834699999.
712	43.9198868560001, −90.281512146.	44.2491740180001, −90.281512146.	44.2491740180001, −89.9961840639999.	43.9198868560001, −89.9961840639999.
713	42.308018614, −85.261730616.	42.319058737, −85.261730616.	42.319058737, −85.241088866.	42.308018614, −85.241088866.
714	43.1194738070001, −87.9811739899999.	43.1294331440001, −87.9811739899999.	43.1294331440001, −87.969765633.	43.1194738070001, −87.969765633.
715	21.444134852, −158.193880164.	21.449106118, −158.193880164.	21.449106118, −158.188834873.	21.444134852, −158.188834873.
716	33.30623532, −116.726204555.	33.348258648, −116.726204555.	33.348258648, −116.681746107.	33.30623532, −116.681746107.
717	40.416741642, −74.074863319.	40.428227856, −74.074863319.	40.428227856, −74.066019589.	40.416741642, −74.066019589.
718	42.715762833, −73.715197659.	42.723757367, −73.715197659.	42.723757367, −73.7014418059999.	42.715762833, −73.7014418059999.
719	38.131610059, −76.4415151439999.	38.158782096, −76.4415151439999.	38.158782096, −76.4141914209999.	38.131610059, −76.4141914209999.
720	29.9448494910001, −90.0376652149999.	29.9527562370001, −90.0376652149999.	29.9527562370001, −90.028618848.	29.9448494910001, −90.028618848.
721	39.905374947, −113.701870713.	40.419222199, −113.701870713.	40.419222199, −112.723055564.	39.905374947, −112.723055564.
722	41.3164009720001, −74.104566558.	41.4138497160001, −74.104566558.	41.4138497160001, −73.950569356.	41.3164009720001, −73.950569356.
723	42.1732117120001, −72.560346443.	42.2183966200001, −72.560346443.	42.2183966200001, −72.513149263.	42.1732117120001, −72.513149263.
724	21.4548202730001, −158.05113405.	21.4906567190001, −158.05113405.	21.4906567190001, −158.023893229.	21.4548202730001, −158.023893229.

TABLE 1 TO § 202.1401—Continued

Area ID				
725	47.6996152880001, −117.582780473.	47.7046436220001, −117.582780473.	47.7046436220001, −117.571913796.	47.6996152880001, −117.571913796.
726	32.3256631690001, −106.751912813.	33.9110868210001, −106.751912813.	33.9110868210001, −106.097200035.	32.3256631690001, −106.097200035.
727	38.7024149040001, −93.5961699699999.	38.7611248150001, −93.5961699699999.	38.7611248150001, −93.530993696.	38.7024149040001, −93.530993696.
728	35.403434766, −97.615579224.	35.411418204, −97.615579224.	35.411418204, −97.607653269.	35.403434766, −97.607653269.
729	30.5215171080001, −88.98512068.	30.5592917870001, −88.98512068.	30.5592917870001, −88.952736979.	30.5215171080001, −88.952736979.
730	39.7790113880001, −84.122505244.	39.8514988460001, −84.122505244.	39.8514988460001, −84.013795999.	39.7790113880001, −84.013795999.
731	28.235254233, −98.748507381.	28.257299957, −98.748507381.	28.257299957, −98.699312525.	28.235254233, −98.699312525.
732	34.8723464400001, −116.88720812.	34.9011810040001, −116.88720812.	34.9011810040001, −116.849270991.	34.8723464400001, −116.849270991.
733	37.211273261, −76.4914782399999.	37.220744848, −76.4914782399999.	37.220744848, −76.4804938719999.	37.211273261, −76.4804938719999.
734	41.2592384490001, −80.6956297689999.	41.2720857920001, −80.6956297689999.	41.2720857920001, −80.6669307879999.	41.2592384490001, −80.6669307879999.
735	64.7319686270001, −147.051773314.	64.8134110040001, −147.051773314.	64.8134110040001, −146.755123322.	64.7319686270001, −146.755123322.
736	32.765238373, −114.588551663.	33.551544978, −114.588551663.	33.551544978, −113.648148435.	32.765238373, −113.648148435.

Dated: December 26, 2024.

Matthew G. Olsen,

Assistant Attorney General for National Security, U.S. Department of Justice.

[FR Doc. 2024–31486 Filed 1–3–25; 8:45 am]

BILLING CODE 4410–PF–P