Department of Justice

April 11, 2025
www.justice.gov

National Security Division
Foreign Investment Review Section

DATA SECURITY PROGRAM:
FREQUENTLY ASKED QUESTIONS

Overview

The Data Security Program ("DSP") implemented by the National Security Division ("NSD") under Executive Order 14117 comprehensively and proactively addresses the continued efforts of foreign adversaries to use commercial activities to access, exploit, and weaponize U.S. Government-related data and Americans' bulk sensitive personal data.

On January 8, 2025, NSD issued a final rule implementing Executive Order 14117, which is now available at 28 CFR Part 202. Unless otherwise indicated, all citations are to the sections of the DSP regulations in 28 CFR Part 202. These Frequently Asked Questions ("FAQs") address high-level clarifications about Executive Order 14117 and the DSP. NSD, which implements the DSP primarily through the Foreign Investment Review Section, will periodically update this list of FAQs with additional questions and answers. You can request that NSD provide an answer to a new question by emailing nsd.firs.datasecurity@usdoj.gov with the subject "FAQ request." Please note, however, that any information submitted concerning FAQs may not necessarily be treated as confidential or proprietary to the submitter, and any information may be subject to disclosure under the Freedom of Information Act and similar laws.

The questions and answers are intended only as general information to assist individuals and entities in complying with legal requirements and to facilitate an understanding of the scope and purposes of the DSP. U.S. businesses, individuals, and others subject to U.S. jurisdiction must comply with the full legal requirements of the DSP, which are set forth in the applicable statutes, Executive Orders, and implementing regulations in 28 CFR part 202. These FAQs do not alter those legal requirements. To the extent that there is any apparent inconsistency between these FAQs and IEEPA, Executive Order 14117, or the implementing regulations, the latter control. The reader is further cautioned that specific facts may alter an analysis and, because each scenario may reflect unique foreign policy and national security contexts, a particular answer may not be universally applicable to all circumstances.

These FAQs do not create any privileges, benefits, or rights, substantive or procedural, enforceable at law or in equity by any individual, organization, party, or witness in any administrative, civil, criminal, or other matter.

Basic Program Information

1. What does Executive Order 14117 (Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern) do? What does the DSP do?

E.O. 14117, in part, directs the Department 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 U.S. Government-related data ("government-related data") or bulk U.S. sensitive personal data, as defined by final rules implementing E.O. 14117; is a member of a class of transactions that has been determined by the Department 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 bulk sensitive personal data; and meets other criteria specified by E.O. 14117. To implement E.O. 14117, the final rule, as codified at 28 CFR part 202, identifies classes of prohibited and restricted transactions ("covered data transactions") and exempted transactions; identifies countries of concern and classes of covered persons; defines key terms, identifies numeric thresholds above which a data set is considered bulk, establishes a process to issue (including to modify or rescind) general and specific licenses authorizing otherwise prohibited or restricted transactions and to issue advisory opinions; and addresses recordkeeping and reporting of transactions to inform NSD's investigative, enforcement, and regulatory efforts.

Issued on April 11, 2025.

2. Who must comply with the DSP?

NSD expects U.S. persons to know their transactions and data. Specifically, U.S. persons should have awareness of the type and volume of their data and whether they maintain or deal in government-related data and bulk U.S. sensitive personal data. U.S. persons that choose to engage in covered data transactions with this kind of data and that conduct business with covered persons or countries of concern must comply with the DSP. Non-U.S. persons are also subject to certain DSP prohibitions. For example, the § 202.304 prohibition on evasions, attempts, causing violations, and conspiracies applies to all persons, including non-U.S. persons, and prohibits, among other things, causing a violation of the prohibitions, conspiracies formed to violate the prohibitions, as well as engaging in conduct that evades the DSP.

Issued on April 11, 2025.

3. What was the process for establishing the DSP?

The process involved extensive consultation with and input from the private sector, foreign partners, and other stakeholders. E.O. 14117 involved significant informal consultation with hundreds of private-sector and foreign partners before it was issued. After its issuance, NSD voluntarily undertook two rounds of formal opportunities for the public to provide feedback before issuing the final rule. On March 5, 2024, the Department published an Advance Notice of Proposed Rulemaking ("ANPRM") in the Federal Register that set forth the contemplated contours of the rule, posed 114 specific questions for public input, and allotted 45 days for public comment. The Department also solicited informal input on the ANPRM through dozens of large group listening sessions, industry engagements, and one-on-one engagements with hundreds of participants. The Department also, both on its own and with other agencies, met with businesses, trade groups, and other stakeholders interested in or impacted by the contemplated regulations to discuss the ANPRM. The Department received 64 timely comments on the ANPRM. 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.

The Department carefully considered the comments on the ANPRM in subsequently preparing a Notice of Proposed Rulemaking ("NPRM"), which was published in the Federal Register on October 29, 2024 with a 31-day public comment period. During the NPRM comment period, the Department, both on its own and with other agencies, met with businesses, trade groups, and other stakeholders interested in or impacted by the contemplated regulations to discuss the NPRM. During the NPRM comment period, the Department, in coordination with the Department of Commerce, conducted individual consultations with several trade associations. The Department then carefully considered public comments on the NPRM from trade associations, public interest advocacy groups, think tanks, private individuals, and companies, as well as comments from several foreign governments. Although the NPRM evolved from the ANPRM based on the Department's consideration of public comments, such as by adding new 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. The Department received and carefully reviewed 75 timely comments on the NPRM.

The Department issued the final rule on January 8, 2025.

Issued on April 11, 2025.

4. What is the effective date for the DSP?

NSD recognizes that individuals and companies may need to take steps to determine whether the DSP's prohibitions and restrictions apply to their activities, and to implement changes to their existing policies or to implement new policies and processes to comply. These steps may vary greatly depending on the existing structure and commercial activities of the entities subject to the DSP, but could include revising or creating new internal policies and processes, identifying data flows, changing vendors or suppliers, adjusting employee roles or responsibilities, deploying new security requirements, and revising existing contracts.

There are two key effective dates associated with the DSP: April 8, 2025 and October 6, 2025. Starting April 8, 2025, entities and individuals are required to comply with the DSP's prohibitions and restrictions, and with all other provisions of the DSP with the exception of the affirmative obligations of subpart J (related to due diligence and audit requirements for restricted transactions), § 202.1103 (related to reporting requirements for certain restricted transactions), and § 202.1104 (related to reports on rejected prohibited transactions). Starting October 6, 2025, entities and individuals must comply with subpart J and §§ 202.1103 and 202.1104. These effective dates remain in force.

However, consistent with the Executive's Article II authority to exercise enforcement discretion, NSD will target its enforcement efforts during the first 90 days to allow U.S. persons (e.g., individuals and companies) additional time to continue implementing the necessary changes to comply with the DSP and provide additional opportunities for the public to engage with NSD on DSP-related inquiries. Specifically, NSD will not prioritize civil enforcement actions against any person for violations of the DSP that occur from April 8 through July 8, 2025 so long as the person is engaging in good faith efforts to comply with or come into compliance with the DSP during that time. These efforts include engaging in activities enumerated in NSD's Data Security Program Implementation and Enforcement Policy Through July 8, 2025, including amending or renegotiating existing contracts, conducting internal reviews of data flows, deploying the CISA security measures, etc.

This policy aims to allow the private sector to focus its resources and efforts on promptly coming into compliance and to allow NSD to prioritize its resources on facilitating compliance. This policy does not restrict NSD's lawful authority and discretion to pursue criminal enforcement in cases where individuals or entities willfully violate, attempt to violate, conspire to violate, cause a violation of, or engage in any action intended to evade or avoid the DSP's requirements.

During this 90-day period, NSD encourages the public to contact NSD at nsd.firs.datasecurity@usdoj.gov with informal inquires or information about the DSP and the guidance NSD has released. Although NSD may not be able to respond to every inquiry, NSD will use its best efforts to respond consistent with available resources, and any inquiries or information submitted may be used to develop and refine future guidance. Correspondingly, NSD discourages the submission of any formal requests for specific licenses or advisory opinions during this 90-day period: Although requests for specific licenses or advisory opinions during this 90-day period can be submitted, NSD will not review or adjudicate those submissions

during the 90-day period (absent an emergency or imminent threat to public safety or national security).

At the end of this 90-day period, individuals and entities should be in full compliance with the DSP and should expect NSD to pursue appropriate enforcement with respect to any violations.

Issued on April 11, 2025.

5. Do the prohibitions of the DSP apply in instances where a U.S person gives access to government-related or bulk U.S. sensitive personal data to another U.S. person?

Generally, no. The DSP does not address purely domestic data 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 designated as covered persons.

Issued on April 11, 2025.

6. Do the prohibitions of the DSP apply in instances where a covered person gives access to government-related or bulk U.S. sensitive personal data to a U.S. person?

No. A U.S. person accessing data from a covered person ordinarily does not present the national security concerns that the DSP seeks to address, and NSD does not intend the DSP to cover that generic circumstance. The definition of "covered data transaction" captures only those transactions that involve access by a country of concern or covered person to government-related data or bulk U.S. sensitive personal data (as the term "access" is defined in the DSP)—not the other way around. As a result, the DSP does not impose any restrictions or prohibitions on transactions that do not involve the risk of a country of concern or covered person obtaining access to government-related data or bulk U.S. sensitive personal data.

Issued on April 11, 2025.

7. Does the DSP give NSD new surveillance authorities or the ability to track Americans' data?

No. The DSP has nothing to do with the U.S. Government's authorities to lawfully engage in law enforcement and national security activities to gather intelligence. Nothing in the DSP, on its face or in practice, requires U.S. companies to surveil their employees, customers, or other private entities, or to submit Americans' sensitive personal data to the U.S. Government. As the final rule explained, the DSP generally requires that persons subject to U.S. jurisdiction have and implement a compliance program tailored to their individualized risk profile—a common feature of sanctions, export controls, anti-money laundering, privacy, and national security and other laws. Effective October 6, 2025, the DSP will also require that U.S. persons engaged in restricted transactions conduct certain affirmative due diligence to monitor their own transactions, double-

check their compliance, and identify areas of noncompliance. Moreover, the DSP categorically exempts the regulation of transactions to the extent they involve expressive materials, informational materials, or personal communications under 50 U.S.C. § 1702(b)(1) and (b)(3).

Issued on April 11, 2025.

8. How does the DSP interact with the Committee on Foreign Investment in the United States (CFIUS)?

The DSP prescribes prospective and categorical rules to regulate a set of commercial transactions and relationships that afford countries of concern or covered persons with access to government-related data or bulk U.S. sensitive personal data, including non-passive investment agreements.

Generally, where a transaction involves an investment agreement that is also a covered transaction subject to CFIUS's review, the DSP's security requirements regulating U.S. persons' engagement in a restricted transaction apply until and unless CFIUS takes certain actions to address the data security risks, like entering into a National Security Agreement (NSA). If CFIUS enters into a mitigation agreement that imposes data security-related mitigation, then the requirements of the DSP would no longer apply, and the obligations under the CFIUS NSA would take over, to avoid duplicative or overlapping requirements. Importantly, CFIUS would have to explicitly designate its action as a "CFIUS action"—making clear when an investment agreement is subject to the DSP or CFIUS.

Issued on April 11, 2025.

9. How does the DSP interact with the Department of Commerce's Office of Information and Communications Technology and Services (ICTS)?

Generally, ICTS authorities focus on transactions that involve information and communications technology or services designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries and that otherwise pose an unacceptable risk to U.S. national security. The DSP prescribes forward-looking, categorical rules (including security requirements) across certain vendor agreements, some of which could also be subject to an action by the Department of Commerce using its ICTS authorities under E.O. 13873. In these instances, the DSP's security requirements create a floor for the security of all government-related data or bulk U.S. sensitive personal data involved in such a vendor agreement, while still allowing Commerce to take more stringent actions against a specific vendor, transaction, or class of ICTS beyond those requirements established by the DSP.

Issued on April 11, 2025.

10. How does the DSP align with economic sanctions and export controls?

Economic sanctions and export controls are generally used to address the transfer of funds, material support, sensitive U.S. products, and technologies to prevent foreign adversaries and certain other countries from acquiring and using them for malign purposes, but they do not address the flow of sensitive personal data as defined in the DSP or the counterintelligence and related risks posed by such data. The DSP, economic sanctions, and export controls generally are (or have been) based on IEEPA authorities. The DSP's regulation of transactions is targeted to prohibiting or restricting specific classes of transactions with covered persons or countries of concern. By contrast, many sanctions programs prohibit all transactions and dealings with persons on the Specially Designated National and Blocked Persons List, unless exempt or otherwise authorized.

Issued on April 11, 2025.

11. Does the DSP prohibit all data transactions between the United States and all foreign persons or all foreign countries?

No. The DSP generally governs covered data transactions with, or that involve access by, covered persons or countries of concern. There are only two limited instances in which the DSP governs data transactions between U.S. persons and third countries (i.e., a transaction in which a country of concern or covered person is not a party). First, to prevent the resale or onward transfer of government-related data or bulk sensitive personal data to countries of concern or covered persons, the DSP imposes some conditions on U.S. persons engaging in covered data transactions involving data brokerage with foreign persons that are not covered persons. (See FAQ 62). Second, the DSP prohibits 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—which could include, for example, attempts to evade the DSP's prohibitions by using foreign persons or foreign governments as proxies for covered persons or countries of concern.

Issued on April 11, 2025.

12. How does the DSP compare to the Protecting Americans' Data from Foreign Adversaries Act of 2024 (PADFAA)?

The PADFAA generally makes it unlawful for a "data broker to sell" or "otherwise make available personally identifiable sensitive data of a United States individual" to any foreign adversary country or any entity that is controlled by a foreign adversary and authorizes the Federal Trade Commission ("FTC") to bring civil enforcement actions for any violations. *See* Pub. L. 118-50, div. I, 138 Stat. 895, 960 (2024). As explained in the DSP NPRM and final rule, there are significant differences in scope and structure between the PADFAA and the DSP. For example:

- ***Enforcement.*** PADFAA is enforced by the FTC using case-by-case, retrospective enforcement actions. The DSP establishes comprehensive set of transparent, predictable, and prospective rules.
- ***Types of data.*** The DSP covers six categories of sensitive personal data (human 'omic data and associated biospecimens, human biometric data, precise geolocation data, personal health data, personal financial data, and covered personal identifiers). PADFAA generally covers broader types of data, such as photos, videos, audio recordings, information identifying an individual's sexual behavior, information about minors, and an individual's private communications.
- ***What is covered.*** PADFAA applies only to the activities of a certain kind of entity (third-party "data brokers"). The DSP applies to classes of activities engaged in by any U.S. person, including all forms of data brokerage (including first- and third-party data brokerage), that present the national-security risk of allowing countries of concern or covered persons access to sensitive personal data, regardless of the kinds of entities or individuals who engage in that activity.
- ***Countries of concern.*** PADFAA covers China, Iran, North Korea, and Russia, whereas the DSP designates those same countries, plus Venezuela and Cuba, as countries of concern.
- ***Third-party re-export.*** Unlike the DSP, PADFAA does not expressly address the re-export or resale of data by third parties and indirect sales through intermediaries to countries of concern.
- ***Consent-based exception.*** PADFAA's prohibition does not apply to the extent that a data broker transmits a U.S. individual's data at that individual's request or direction. The DSP does not contain any such consent-based exception in light of the national security threat posed even in such instances.
- ***Mechanisms for redress.*** PADFAA does not provide any mechanisms for affected parties to seek clarification or redress, such as the advisory opinions, general licenses, and specific licenses available to parties under the DSP.

Issued on April 11, 2025.

Program Elements

13. What are the countries of concern?

The Department has identified the following countries of concern:

- The People's Republic of China ("PRC"), including the Special Administrative Region of Hong Kong and the Special Administrative Region of Macau;
- The Russian Federation;
- The Islamic Republic of Iran;
- The Democratic People's Republic of Korea;
- The Republic of Cuba; and

- The Bolivarian Republic of Venezuela

These countries (1) 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 (2) pose a significant risk of exploiting bulk U.S. sensitive personal data or government-related data to the detriment of the national security of the United States or security and safety of U.S. persons.

Issued on April 11, 2025.

14. What is a covered person?

A covered person is an individual or entity that either falls into one of the DSP's categories of covered persons, or that NSD has designated as a covered person. Under § 202.211(a), the four self-executing categories of covered persons, which exclude U.S. persons, are: (1) foreign entities headquartered in or organized under the laws of a country of concern; (2) foreign entities 50% or more owned by a country of concern or covered person; (3) foreign individuals primarily resident in a country of concern; and (4) foreign individuals who are employees or contractors of a covered person entity or a country-of-concern government. Any person falling into one or more of these categories is automatically a covered person without further action by NSD. To assist in compliance, however, NSD may choose to publicly identify some covered persons in those categories on its Covered Persons List. The identification of such covered persons, however, does not eliminate U.S. persons' obligation to take reasonable steps, as part of a risk-based compliance program, to ascertain whether other individuals and entities fall into one or more of those categories of covered persons.

Under § 202.211(a)(5), NSD may also designate any person (including a U.S. person) as a covered person upon determining that the persons meets certain listed criteria, such as being subject to the ownership or control of a country of concern. NSD will add any designated covered persons to the Covered Persons List. Designated covered persons remain covered persons even when located in the United States.

Issued on April 11, 2025.

15. What is a covered data transaction?

A covered data transaction is any transaction that involves 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.

Issued on April 11, 2025.

16. What is a prohibited transaction?

Under § 202.244, the term "prohibited transaction" means a data transaction involving access by a country of concern or covered person that is subject to one or more of the prohibitions described in DSP subpart C. There are five categories of prohibited transactions.

- U.S. persons knowingly engaging in a covered data transaction involving data brokerage with a country of concern or covered person (§ 202.301)
- U.S. persons knowingly engaging in a covered data transaction involving data brokerage with a foreign person (that is not a covered person) *unless* the U.S. person (1) contractually requires that the foreign person refrain from onward sale with a country of concern or covered person; and (2) reports any known or suspected violations of this contractual requirement (§ 202.302)
- U.S. persons knowingly engaging in a covered data transaction with a country of concern or covered person that involves access by that country of concern or covered person to bulk human 'omic data, or to human biospecimens from which bulk human 'omic data could be derived (§ 202.303)
- Transactions with the purpose of evading or avoiding, causes a violation of, or attempts to violate any of the prohibitions set forth in the DSP or any conspiracy formed to violate the prohibitions in the DSP (§ 202.304)
- U.S. persons knowingly directing any covered data transaction that would be a prohibited transaction or unauthorized restricted transaction if engaged in by a U.S. person

Issued on April 11, 2025.

17. What is a restricted transaction?

Under § 202.246, the term "restricted transaction" means a transaction subject to the restrictions in subpart D. U.S. persons are prohibited from knowingly engaging in a covered data transaction involving a vendor agreement, employment agreement, or investment agreement with a country of concern or covered person (a "restricted transaction"), unless the U.S. person complies with Cybersecurity and Infrastructure Security Agency ("CISA") security requirements and other applicable requirements. If a U.S. person engages in a restricted transaction without complying with the security requirements and other applicable requirements, such activity would be considered an unauthorized restricted transaction and a violation of the DSP, pursuant to § 202.304.

Covered data transactions that involve a vendor, employment, or investment agreement and involve access by countries of concern or covered persons to bulk human genomic data or human biospecimens from which such data can be derived are prohibited transactions—not restricted transactions—and are subject to the prohibitions in § 202.303.

Issued on April 11, 2025.

18. What is data brokerage?

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. This definition covers both first-party data brokerage (by the person that directly collected the U.S. person's data) and third-party data brokerage (by a person that did not directly collect the U.S. person's data, such as a subsequent reseller).

Issued on April 11, 2025.

19. Which general types of data do E.O. 14117 and the DSP protect?

Among other things, E.O. 14117 directed the Department 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.

Issued on April 11, 2025.

20. What are the categories of sensitive personal data?

There are six categories of "sensitive personal data" that could be exploited by a country of concern or covered person 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. The categories are: (1) covered personal identifiers; (2) precise geolocation data; (3) biometric identifiers; (4) human 'omic data; (5) personal health data; and (6) personal financial data.

Issued on April 11, 2025.

21. What are covered personal identifiers?

Covered personal identifiers are 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. There are two subcategories of covered personal identifiers. First, listed identifiers in combination with any other listed identifier. Second, 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. This category excludes 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 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.

Under the DSP, IP addresses, which can be useful in narrowing down, and thus increasing the identifiability of, other data that is linked or linkable to a U.S. person, are covered personal identifiers (not precise geolocation data).

Issued on April 11, 2025.

22. Does the definition of bulk U.S. sensitive personal data exclude data that has been anonymized, de-identified, pseudonymized, or aggregated?

No. 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. Even anonymized data, when aggregated, can still be used by countries of concern and covered persons to identify individuals and to conduct malicious activities that implicate the risk to national security E.O. 14117 was intended to address. The DSP includes sensitive personal data that is anonymized, pseudonymized, de-identified, or encrypted 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 DSP's other applicable requirements.

Issued on April 11, 2025.

23. What is precise geolocation data?

Precise geolocation data is 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. *See* § 202.242.

Issued on April 11, 2025.

24. What are biometric identifiers?

Biometric identifiers are 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. *See* § 202.204.

Issued on April 11, 2025.

25. What is human 'omic data?

Human 'omic data includes human genomic data (for more information, see FAQ 26), human epigenomic data (for more information, see FAQ 27), human proteomic data (for more information see FAQ 28), and human transcriptomic data (for more information, see FAQ 29). This category excludes pathogen-specific data embedded in human 'omic data sets. *See* § 202.224.

Issued on April 11, 2025.

26. What is human genomic data?

Human genomic data is data representing the nucleic acid sequences that constitute the entire set or a subset of the genetic instructions within a human cell. This includes results from an individual's genetic test and any related human genetic sequencing data. *See* § 202.224(a)(1).

Issued on April 11, 2025.

27. What is human epigenomic data?

Human epigenomic data is 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. *See* § 202.224(a)(2).

Issued on April 11, 2025.

28. What is human proteomic data?

Human proteomic data is 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. *See* § 202.224(a)(3).

Issued on April 11, 2025.

29. What is human transcriptomic data?

Human transcriptomic data is 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. *See* § 202.224(a)(4).

Issued on April 11, 2025.

30. What is personal health data?

This is 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. *See* § 202.241.

Issued on April 11, 2025.

31. Is personal health data limited to data involved in transactions with, or collected or held by, medical and healthcare professionals and institutions?

No. Personal health data, as defined in § 202.241, is not limited to data collected only by medical and healthcare professionals and institutions. Instead, the term personal health data applies to any data that meets the definition regardless of the entity that collects or holds it, and regardless of the type of transaction in which that data is involved. For example, it includes logs of exercise habits, which could be collected by fitness apps. The DSP's definition of "personal health data" is therefore different in that respect than the definition of "health information" under the Health

Insurance Portability and Accountability Act of 1996, which is defined by the type of entity that receives or creates it. *See* 45 CFR 160.103.

Issued on April 11, 2025.

32. What is personal financial data?

This 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)). *See* § 202.240.

Issued on April 11, 2025.

33. Does the definition of personal financial data include inferences about that data? For example, while a hotel record transaction may be personal financial data, is an ultimate inference that the person is interested in business travel considered personal financial data?

The DSP prohibits or restricts only certain categories of transactions in bulk U.S. sensitive personal data and government-related data, neither of which include inferences on their own.

Issued on April 11, 2025.

34. Does personal financial history only pertain to transactions with financial institutions?

No. Personal financial data, as defined in § 202.240, includes payment history but is not limited to purchases and payment history collected only by financial institutions. It includes all purchase and payment history. 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.

Issued on April 11, 2025.

35. What is U.S. Government-related ("government-related") data?

There are two types of government-related data. The first is any precise geolocation data, regardless of volume, for any location within any area enumerated on the Government-Related Location Data List in § 202.1401. The listed locations include certain worksites or duty stations of U.S. Government employees or contractors occupying national security positions, certain military installations, and certain facilities or locations that otherwise support the U.S.

Government's national security, defense, intelligence, law enforcement, or foreign policy missions.

The second type of government-related data is 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. 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. 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.

Issued on April 11, 2025.

36. What is an example of sensitive personal data that is marketed as linked or linkable to current or recent former U.S. Government employees, contractors, or former senior officials in such a way that it constitutes government-related data?

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 because the transaction party has marketed the information 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. *See* § 202.222(b) for additional examples.

Issued on April 11, 2025.

37. What are the bulk thresholds for U.S. sensitive personal data?

The table below summarizes the bulk thresholds for sensitive personal data. Sensitive personal data meeting or exceeding these thresholds at any point in the preceding twelve 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, is bulk U.S. sensitive personal data:

U.S. Sensitive Personal Data	**Threshold of data collected about or maintained on…**
Human genomic data	100 U.S. persons
Human epigenomic data	1,000 U.S. persons
Human proteomic data	1,000 U.S. persons
Human transcriptomic data	1,000 U.S. persons
Biometric identifiers	1,000 U.S. persons

Precise geolocation data	1,000 U.S. devices
Personal health data	10,000 U.S. persons
Personal financial data	10,000 U.S. persons
Covered personal identifiers	100,000 U.S. persons
Combined data, as described in § 202.205(g)	Lowest applicable number

Issued on April 11, 2025.

38. For the purposes of determining whether a category of U.S. sensitive personal data meets the bulk threshold, does the "preceding twelve months" include time that elapsed before the relevant DSP effective date?

No. The DSP regulates covered data transactions initiated, pending, or completed on or after the applicable effective date. As such, U.S. persons should only consider covered data transactions "in the preceding twelve months" that occur on or after the effective date of the DSP. For more information about the DSP's effective dates, see FAQ 4.

Issued on April 11, 2025.

39. Are there exceptions to the DSP's prohibitions?

Yes. Exemptions to the prohibitions and restrictions of the DSP include:

- 202.501 – Personal communications.
- 202.502 – Information or informational materials.
- 202.503 – Travel.
- 202.504 – Official business of the United States Government.
- 202.505 – Financial services.
- 202.506 – Corporate group transactions.
- 202.507 – Transactions required or authorized by Federal law or international agreements, or necessary for compliance with Federal law.
- 202.508 – Investment agreements subject to a CFIUS action.
- 202.509 – Telecommunications services.
- 202.510 – Drug, biological product, and medical device authorizations.
- 202.511 – Other clinical investigations and post-marketing surveillance data.

As necessary and appropriate, NSD may also issue general or specific licenses to authorize certain transactions that would otherwise be prohibited. For guidance on how to request and apply for a specific license, please see § 202.802.

Issued on April 11, 2025.

40. What is a general license?

A license is an authorization from NSD to engage in a prohibited or restricted transaction. There are two types of licenses: general licenses and specific licenses. Either license may be revoked or modified at any time at the discretion of NSD.

A general license authorizes a particular type of transaction for a class of persons. General licenses are self-executing, meaning they allow persons to engage in certain transactions involving the United States or U.S. persons without needing to apply for a specific license, provided the transactions meet certain terms and conditions as described in the general license. Persons cannot apply for a general license.

General licenses (1) do not excuse compliance with any law or regulation administered by another agency (including reporting requirements applicable to the transactions and activities therein licensed), (2) do not release the licensees or third parties from civil or criminal liability for violation of any law or regulation, and (3) do not constitute a finding of fact or conclusion of law with respect to the applicability of any law or regulation.

Issued on April 11, 2025.

41. What is a specific license?

A license is an authorization from NSD to engage in a prohibited or restricted transaction. There are two types of licenses: general licenses and specific licenses. Either license may be revoked or modified at any time at the discretion of NSD.

NSD may issue a specific license to particular individuals or entities, authorizing a particular transaction or transactions in response to a written license application. A specific license is not transferable, is limited to the facts and circumstances specific to the application, and is subject to the provisions of the DSP and Executive Order 14117.

Persons engaging in transactions pursuant to specific licenses must make sure that all conditions of the licenses are strictly observed, including reporting requirements. NSD may, at its discretion, declare a specific license void from the date of its issuance, or from any other date, if a specific license was issued as a result of willful misrepresentation on the part of the applicant or the applicant's agent.

Specific licenses (1) do not excuse compliance with any law or regulation administered by another agency (including reporting requirements applicable to the transactions and activities therein licensed), (2) do not release the licensees or third parties from civil or criminal liability for violation of any law or regulation, and (3) do not constitute a finding of fact or conclusion of law with respect to the applicability of any law or regulation.

Issued on April 11, 2025.

Covered Persons List

42. What list does NSD maintain for covered persons? Where can I find this list?

NSD publishes the Covered Persons List, which contains (1) an exhaustive list of all individuals and entities that NSD has designated as covered persons under § 202.211(a)(5), and (2) a non-exhaustive list of individuals and entities that NSD has identified as covered persons falling into the categories of § 202.211(a)(1)–(4). This list will be available on NSD's website and will be regularly updated as NSD makes new designations. The Covered Persons List is not exhaustive with respect to persons who fall into the categories of covered persons in § 202.211(a)(1) and thus may not include all persons who meet those criteria, such as entities that are owned 50% or more by a covered person. U.S. persons should do due diligence to determine if they are engaging in a covered data transaction with a covered person.

Issued on April 11, 2025.

43. Is the NSD's Covered Persons List an exhaustive list of all covered persons?

Yes with respect to covered persons designated under § 202.211(a)(5), but no with respect to covered persons identified as falling within one or more categories in § 202.211(a)(1)-(4). Covered persons falling in the categories of §§ 202.211(a)(1)-(4) do not require identification or designation by the Department. Their status as a covered person is based on meeting the defined criteria. Covered persons meeting the criteria of §§ 202.211(a)(1)-(4) will not appear on the Covered Persons List except to the extent that NSD opts to identify them to assist in compliance or separately designates them under § 202.211(a)(5). As a result, entities that are covered persons because they are owned 50% or more by a covered person may not appear on the Covered Persons List. U.S. companies should thus conduct due diligence on the persons with which they do business to determine not only whether they appear as identified or designated covered persons on the Covered Persons List but also whether they are foreign persons that fall within one or more of the categories of covered persons in § 202.211(a)(1)–(4).

Issued on April 11, 2025.

44. How can I get a copy of the Covered Persons List?

The names of persons identified or designated as a covered person are published in the Federal Register and incorporated into the NSD's Covered Persons List. The Covered Persons List is accessible through the NSD website.

Issued on April 11, 2025.

45. How often will the Covered Persons List be updated?

Although there is no predetermined timetable, NSD will periodically update the Covered Persons List as appropriate, including when NSD adds or removes covered persons. Updates to the Covered Persons List will generally be posted on the Data Security Program's website and published in the Federal Register. Publication in the Federal Register is deemed to provide constructive knowledge of a person's status as a covered person that has been designated pursuant to § 202.211(a)(5).

Issued on April 11, 2025.

46. What do I do if I have a match to the Covered Persons List?

If you have checked a name manually or by using software and find a potential match to a person appearing on the Covered Persons List, you should do additional research to verify the person or entity's status. For example, is it an exact name match or very close? Is your customer located in the same general area as the covered person or another entry on the Covered Persons List? If not, it may be a "false hit." The DSP does not prescribe or endorse any specific method to screen counterparties to determine their status as covered persons. Consistent with the DSP, 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.

Issued on April 11, 2025.

47. How can a person seek to be removed from the Covered Persons List?

Consistent with the DSP, persons may seek administrative reconsideration of their status as a designated covered person. NSD will release more information concerning the process for seeking such removal. Please refer to the removal petition procedures set forth in § 202.702.

Issued on April 11, 2025.

48. Are U.S. persons prohibited from engaging in all transactions and dealings with covered persons, similar to the economic sanctions prohibitions administered by the Department of the Treasury's Office of Foreign Assets Control?

No. The prohibitions and restrictions of the DSP are not so broad that they prohibit or restrict all transactions and dealings with covered persons. U.S. persons are prohibited or restricted only from engaging in covered data transactions with covered persons, as specified in subparts C and D of the DSP.

Issued on April 11, 2025.

49. Can U.S. financial institutions open or maintain a bank account for a covered person?

U.S. financial institutions should review § 202.505 for details about the scope of the financial-services exemption. The prohibitions of the DSP generally do not prohibit opening or maintaining a bank account for a covered person. U.S. persons are prohibited or restricted only from engaging in covered data transactions with covered persons as specified in subparts C and D of the DSP. The DSP does not modify or alter any other Federal law or regulation (such as economic sanctions programs) that may affect U.S. persons' ability to open or maintain a bank account for a covered person.

Issued on April 11, 2025.

50. Does the DSP require U.S. persons to ascertain the extent to which an entity or individual is subject to the influence or control of a country of concern or covered person?

No. U.S. persons engaged in data transactions have the duty to determine whether entities or individuals with whom they transact meet the definitions of covered persons set forth in § 202.211(a)(1)–(4), none of which include control or influence. NSD 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 the category of covered persons designated pursuant to § 202.211(a)(5), U.S. businesses need only rely on the Covered Persons List when conducting due diligence and application of the 50% rule.

Issued on April 11, 2025.

51. Where a parent company is headquartered in a country of concern, is that company's U.S. branch a U.S. person?

No. Branches of companies are treated as part of their parent companies. Branches are not independent entities. Such a branch would not be organized solely under the laws of the United States and therefore does not meet the definition of U.S. person under § 202.256.

Issued on April 11, 2025.

52. If an individual who is designated as covered person under § 202.211(a)(5) visits the United States, are they a U.S. person and do they remain a covered person while located in the United States?

Yes. A persons located in the United States meets the definition of U.S. person, and a person that has been designated as a covered person under § 202.211(a)(5) remains a covered person

wherever they are located. As such, U.S. persons would still be subject to the applicable prohibitions or restrictions of engaging in covered data transactions with a covered person designated under § 202.211(a)(5), even while that designated covered person is located in the United States.

Issued on April 11, 2025.

53. If a non-designated covered person individual (who falls into the categories in § 202.211(a)(3) or § 202.211(a)(4), but who is not separately designated under § 202.211(a)(5)) visits the United States, are they a U.S. person and do they remain a covered person while located in the United States?

While located in the United States, a non-designated covered person is a U.S. person and correspondingly loses their covered person status because the categories in § 202.211(a)(3) and (a)(4) apply only to a "foreign person." Upon leaving the United States, the non-designated covered person will automatically revert to being a foreign person and a covered person under 202.211(a)(3) or (a)(4). Keep in mind, however, that any attempt to structure an otherwise prohibited or restricted transaction to avoid the DSP's prohibitions, such as by having a covered person enter the United States to receive bulk U.S. sensitive personal data, could constitute evasion and a violation of the DSP. See also FAQ 52.

Issued on April 11, 2025.

54. Would NSD issue certificates of non-inclusion to help prove that a name is not on the Covered Persons list?

No, NSD will not issue any non-inclusion certificates to show that an entity or individual is not a covered person or is not on the Covered Persons List. NSD does not intend to publish a "safe list" or "whitelist." For questions regarding whether a specific entity or individual may be a positive match to an entry on the Covered Persons List, please see FAQ 46.

Issued on April 11, 2025.

55. I have not been designated as a covered person pursuant to § 202.211(a)(5), but I meet one or more of the definitions of covered persons listed in 28 CFR §§ 202.211(a)(1)-(4). Can I petition for removal of my status as a covered person?

No. While NSD may identify some persons who fall within one of the categories of covered persons in § 202.211(a)(1)-(4) on the Covered Persons List to help with compliance, those persons are automatically covered persons by virtue of falling within those categories and not by virtue of NSD's exercise of discretion in identifying them under § 202.211(a)(5). Accordingly, such persons may not petition for removal from the Covered Persons List. Parties may, however, apply for a specific license to conduct a prohibited or restricted transaction with a covered

person, including one that falls within one of the categories in § 202.211(a)(1)–(4). U.S. persons remain subject to the prohibitions and restrictions governing covered data transactions with all covered persons, whether they appear on the Covered Persons List or not.

Issued on April 11, 2025.

56. Does NSD have an email service that will notify me when there are updates to the Covered Persons List?

Yes. NSD has multiple e-mail subscription services available. Please visit the following link to sign up for these services. This feed is updated whenever the DSP site is updated.

Issued on April 11, 2025.

57. Does the DSP aggregate ownership stakes of all covered persons when determining whether an entity is a covered person pursuant to the 50% rule?

Yes. The DSP treats any entity owned in the aggregate, directly or indirectly, at least 50% by one or more covered persons as itself a covered person. For example, if covered person X owns 25% of Entity A, and covered person Y owns another 25% of Entity A, Entity A is a covered person because Entity A is owned 50% or more in the aggregate by one or more covered persons. *See* § 202.211(b) for additional examples.

Issued on April 11, 2025.

58. One or more individuals who are covered persons control, but do not own 50% or more of, Entity A, and Entity A does not otherwise meet the criteria of §§ 202.211(a)(1)-(2). Entity A also has not been designated as a covered person under § 202.211(a)(5). Can U.S. persons engage in covered data transactions with a covered person acting on behalf of Entity A (e.g., where a covered person is an executive of Entity A and is signing a contract on behalf of Entity A)?

No. The covered person's signature, even if on behalf of a non-covered person like Entity A, constitutes a covered data transaction and would fall within the scope of the DSP's prohibitions and restrictions. U.S. persons are expected to conduct reasonable due diligence, as part of a compliance program tailored to their individual risks, on the persons with whom they are conducting data transactions—in this example, the covered person executive of Entity A. However, absent evasion, U.S. persons engaging in vendor agreements and other classes of data transactions with foreign persons are generally not expected to conduct "second-level" due diligence on the employment practices of those foreign persons to determine whether their employees qualify as covered persons, as explained in the final rule. *See* § 202.401, example 3 and § 202.305, example 8.

Issued on April 11, 2025.

59. Does NSD consider entities over which one or more covered persons exercise control, but of which they do not own 50% or more in the aggregate, to be a covered person?

No. A covered person holding a controlling interest may present risks of access, which is why control is one of the criteria for NSD to consider when designating 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%, 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 NSD 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 DSP.

Issued on April 11, 2025.

60. Under §§ 202.211(a)(1)-(2), a foreign person is a covered person if, among other things, it is an entity that is 50% or more owned, directly or indirectly, by a country of concern or a covered person. How does NSD interpret indirect ownership as it relates to certain complex ownership structures?

"Indirectly" generally refers to a person's ownership of shares of an entity through another entity or entities. Consistent with OFAC's 50% rule, when a covered person directly owns 50% or more of an entity, the covered person also indirectly owns what that entity directly owns, as shown by the examples below. By contrast, when a covered person directly owns less than 50% of an entity, the 50% rule reflected by § 202.211(a)(1) and (2) does not apply, and the covered person is not treated as indirectly owning what that entity directly owns. NSD expects and urges persons considering a potential transaction to conduct appropriate due diligence on entities that are party to or involved with a proposed transaction to determine relevant ownership stakes.

As a reminder, companies do not have an obligation to determine control (as opposed to ownership) of the counterparties with which they do business. NSD will make such determinations regarding control through designations of covered persons, which will be published as part of the Covered Persons List. See FAQ 50 for more information.

Example 1: Covered person X owns 50% of Entity A, and Entity A owns 50% of Entity B. Entity B is a covered person for two independent reasons. First, covered person X indirectly owns 50% of Entity B. Second, covered person X's 50% ownership of Entity A makes Entity A a covered person, and Entity A's direct 50% ownership of Entity B in turn makes Entity B a covered person.

Example 2: Covered person X owns 50% of Entity A and 50% of Entity B. Entities A and B each own 25% of Entity C. Entity C is a covered person for two independent reasons. First — because when a covered person directly owns 50% or more of an entity, the covered person also indirectly owns what that entity owns — covered person X indirectly owns, in the aggregate, 50% of Entity C: through its 50% percent ownership of Entity A, covered person X indirectly owns 25% of Entity C; and through its 50% ownership of Entity B, covered person X indirectly owns another 25% of Entity C. When covered person X's indirect ownership of Entity C through Entity A and Entity B is totaled, it equals 50%. Second, Entity C is a covered person due to the 50% aggregate direct ownership by Entities A and B, which are themselves covered persons due to covered person X's 50% ownership of each.

Example 3: Covered person X owns 50% of Entity A and 10% of Entity B. Entity A also owns 40% of Entity B. Entity B is a covered person for two independent reasons. First, through its 50% ownership of Entity A, covered person X indirectly owns 40% of Entity B. When covered Person X's 40% indirect ownership of Entity B is aggregated with covered person X's direct 10% ownership of Entity B, covered person X's total ownership (direct and indirect) of Entity B is 50%. Second, Entity B is also a covered person due to the 50% aggregate direct ownership by covered person X (10%) and Entity A (40%), the latter of which is itself a covered person because it is 50% owned by covered person X.

Example 4: Covered person X owns 50% of Entity A and 25% of Entity B. Entities A and B each own 25% of Entity C. Covered person X's total ownership (direct or indirect, individually or in the aggregate) of Entity C is not 50% or more. Entity C is not a covered person. Although covered person X indirectly owns 25% of Entity C (through covered person X's 50% direct ownership of Entity A), Entity B is not 50% or more owned by covered person X. Therefore, Entity B is not a covered person and covered person X is not considered to indirectly own any of Entity C through covered person X's partial ownership of Entity B. Furthermore, although Entity A is a covered person, Entity A's ownership of Entity C is not 50% or more.

Example 5: Covered person X owns 25% of Entity A and 25% of Entity B. Entities A and B each own 50% of Entity C. Covered person X's total ownership (direct or indirect, individually or in the aggregate) of Entity C is not 50% or more. Entity C is not a covered person. Covered person X's 25% ownership of each of Entity A and Entity B falls short of 50%. Accordingly, neither Entity A nor Entity B is a covered person entity and Covered person X is not considered to indirectly own any of Entity C through its part ownership of Entities A or B.

Issued on April 11, 2025.

61. I am a U.S. person interested in engaging in a covered data brokerage transaction with Foreign Entity A, which falls within one of the categories of covered persons in § 202.211(a)(1)–(2) due to being owned 50% or more by a designated covered person (Person A). Person A then divests their ownership stakes in Foreign Entity A to less than 50% ownership. Is Foreign Entity A still a covered person?

No, unless Entity A is separately designated as a covered person under § 202.211(a)(5). Under the 50% rule, entities are covered persons if they are owned 50% or more, directly or indirectly, individually or in the aggregate, by one or more covered persons or countries of concern. If one or more covered persons or countries of concern divests their ownership stake in a foreign entity such that the resulting combined ownership by covered persons or countries of concern is less than 50%, then the foreign entity in this scenario no longer falls within the categories of covered persons in § 202.211(a)(1)–(2). A covered person or country of concern holding a less-than-50% controlling interest in an entity may still present risks of access, which is why control is one of the criteria for NSD to designate an entity as a covered person under § 202.211(a)(5).

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%, 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 under § 202.211(a)(1)–(2), and such entities may be designated as a covered person by NSD under § 202.211(a)(5) based on the significant controlling interest. Additionally, U.S. persons should be cautious in dealing with such an entity to ensure that they are not engaging in evasion or avoidance of the DSP.

Issued on April 11, 2025.

Prohibited Transactions

62. Can U.S. persons engage in data-brokerage transactions involving bulk U.S. sensitive personal data or U.S. Government-related data with foreign persons who are not covered persons?

Yes. However, to address the risk of an onward transfer of data by foreign third parties to countries of concern or covered persons, the DSP only allows a U.S. person to engage in a covered data transaction involving data-brokerage with a foreign person that is not a covered person if the U.S. person satisfies certain conditions, including (1) using contractual language in which the foreign person agrees not to resell or give access to a country of concern or covered person to the bulk U.S. sensitive personal data or government-related data, and (2) disclosing to NSD any known or suspected violations of this contractual provision.

Issued on April 11, 2025.

63. I am a U.S. person that engages in covered data transactions involving data brokerage. If I include contractual language restricting the use of the bulk U.S. sensitive personal data, can I engage in business with a covered person or country of concern?

No. As stated in § 202.301, except as otherwise authorized pursuant to subparts D or H or any other provision of the DSP, 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. Section 202.302 allows for U.S. persons to engage in contractually-compliant data brokerage transactions with foreign persons so long as those foreign persons are not covered persons.

Issued on April 11, 2025.

64. I am a U.S. person that has declined to engage in a suspected prohibited transaction. Am I able to tell the covered person or country of concern representative that I've rejected their offer and will be reporting it to NSD?

Yes. The DSP permits, but does not require, a U.S. person to notify a counterparty that it has rejected the transaction in accordance with Executive Order 14117 and 28 CFR part 202. The U.S. person must file a report to NSD within 14 days of rejecting the transaction.

Issued on April 11, 2025.

Restricted Transactions

65. Where can I view the Cybersecurity and Infrastructure Security Agency (CISA) security requirements?

Interested parties can view or obtain CISA's security requirements here. Persons with questions about the applicability or interpretation of CISA's security requirements should contact CISA directly by emailing EOSecurityReqs@cisa.dhs.gov.

Issued on April 11, 2025.

66. Are the provisions regulating restricted transactions intended to prevent access to all government-related or bulk U.S. sensitive personal data by covered persons or countries of concern?

Yes. Restricted transactions are classes of transactions that would be prohibited except to the extent they comply with certain conditions, including CISA's security requirements that are designed to mitigate the risk of access to government-related data or bulk U.S. sensitive personal data by countries of concern or covered persons. 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 requirements that, taken together, are sufficient to prevent access to sensitive personal data that is linkable, identifiable, unencrypted, or decryptable by covered persons or countries of concern 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 persons subject to the

DSP 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).

Issued on April 11, 2025.

67. Does the DSP prohibit U.S. persons from hiring citizens of countries of concern, wherever located, or non-Americans living in countries of concern?

No, except in the case of prohibited transactions described in § 202.303. Furthermore, again excluding covered data transactions described in § 202.303, the DSP does not prohibit employment or vendor agreements with individuals in a country of concern or employed by a covered person. Instead, the DSP allows those employment and vendor agreements to go forward so long as the U.S. persons engaged in them comply with certain conditions—most notably, implementing the CISA security requirements to ensure that those covered person employees or vendors 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 countries of concern.

As noted above, covered data transactions that involve a vendor, employment, or investment agreement and involve access by countries of concern or covered persons to bulk human genomic data or human biospecimens from which such data can be derived are prohibited transactions—not restricted transactions—and are subject to the prohibitions in § 202.303.

Issued on April 11, 2025.

68. Does adherence to CISA security requirements cut off a covered person's access to underlying data such that a data transaction would no longer be considered a covered data transaction, and therefore not be subject to the other requirements of the DSP?

No. In defining the term access, § 202.201 explicitly notes that, "[f]or the 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." In other words, deploying the security requirements to prevent a covered person's access to sensitive personal data has no bearing on whether the restricted transaction is still a covered data transaction. Even after the implementation of CISA's security requirements to mitigate the risk of access to the relevant data, U.S. persons would still need to comply with the DSP's other requirements for restricted transactions (such as the affirmative compliance obligations).

Issued on April 11, 2025.

69. Does the DSP's provisions on restricted transactions prevent U.S. persons from hiring, contracting with, or accepting investments from covered persons or countries of concern?

No. For example, an employment agreement that is a restricted transaction would require that the U.S. person implement CISA's security requirements, including data-level requirements that mitigate the risk that the covered person employee may access data that is linkable, identifiable, unencrypted, or decryptable using commonly available technologies. The DSP does not categorically prohibit the U.S. company from offering employment to covered persons.

As a practical matter, NSD 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. 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 entities subject to the DSP 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.

Issued on April 11, 2025.

Exempt Transactions

70. Do the auditing, due-diligence, recordkeeping, and reporting requirements apply to exempt transactions?

Not unless specified as a condition of a specific exemption. 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. For instance, 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. But U.S. persons must comply with the specific conditions of a particular exemption. The exemption in § 202.510 for certain regulatory approval data, for example, is available only to the extent that the U.S. person complies with specified recordkeeping and reporting requirements.

NSD also separately retains its general authority in § 202.1102 to request and subpoena information to the fullest extent permitted by law, including, as appropriate, regarding transactions that may ultimately be exempt under the DSP.

Issued on April 11, 2025.

Information or Informational Materials

71. Does the DSP prohibit the transmission of information or informational materials?

No. The DSP categorically excludes the regulation of transactions to the extent they involve information or informational materials under 50 U.S.C. § 1702(b)(3), such as videos, artwork, and publications. As explained in the NPRM and final rule, 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. § 202.226 lists several exclusions from the definition of information or informational materials, such as data that is technical, functional, or otherwise non-expressive.

Issued on April 11, 2025.

72. Is metadata covered by the definition of sensitive personal data?

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 DSP, regardless of the type of activity (or transaction) involved. As a result, and as noted in § 202.249, metadata that is ordinarily associated with expressive materials, or that is reasonably necessary to enable the transmission or dissemination of expressive materials, is categorically excluded from the scope of the DSP. Metadata that is not ordinarily associated with expressive materials or not reasonably necessary to its transmission or dissemination is covered because regulating that data does not impermissibly prohibit the export of the expressive material itself.

Issued on April 11, 2025.

Official Business of the United States Government

73. Are research projects that receive both Federal and non-Federal funding covered by the DSP's exemptions? Would these exemptions also cover 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?

Yes, to the extent such otherwise covered data transactions are conducted pursuant to a grant, contract, or other agreement with Federal departments and agencies, such transactions are exempt, even if those transactions also involve funding from non-Federal entities. Where the relevant Federal grant does not direct or authorize the covered data transaction, such activity would not be exempt, since it would not be within the scope of the Federal grant. As noted in section II.H of E.O. 14117, the exemption for official business of the U.S. Government exempts grantees and contactors of Federal departments and agencies so that those departments and agencies can pursue grant-based and contract-based conditions to address and mitigate national security risks that countries of concern can access sensitive personal data in transactions related to their agencies' own grants and contracts, without subjecting those grantees and contractors to dual regulation.

Issued on April 11, 2025.

74. Does the DSP exempt non-Federally funded research involving countries of concern or covered persons?

Generally, no. The DSP does not exempt research projects that involve access to government-related data or bulk U.S. sensitive personal data by countries of concern or covered persons. U.S. persons engaged in research that involves (a) government-related data or bulk U.S. sensitive personal data and (b) access by covered persons or countries of concern to such data should carefully review the definitions of covered data transactions in § 202.210 to determine whether any data sharing associated with the research satisfies the definition of a covered data transaction. As the final rule explained, the rule limits the categories of covered data transactions to transactions that are commercial in nature, meaning that they involve some payment or other valuable consideration. 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. And 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. *See* § 202.214(b)(9) and (10) for additional examples.

Such U.S. persons should also carefully review other exemptions in subpart E to determine whether any other exemption would apply to the research project. U.S. persons that wish to engage in any data transaction with a country of concern or covered person that would otherwise qualify as a covered data transaction may apply for a specific license to authorize their research-related covered data transactions.

Issued on April 11, 2025.

Financial Services

75. Does the financial-services exemption include all data transactions that are part of the operations of financial services entities regulated by Federal or State banking or insurance regulators?

No. Financial institutions are not categorically exempt from the DSP. The DSP does not take an entity-based approach. Instead, the DSP takes an activity-based approach that prohibits, restricts, and exempts certain commercial activities or transactions that pose an unacceptable national security risk, without respect to the kind of entity that engages in them. See § 202.505(b)(12) as an example. The financial-services exemption applies only to data transactions to the extent they are ordinarily incident to and part of the provision of financial services, including financial services described in § 202.505(a)(1)-(6). U.S. persons must 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. For example, an employment agreement (including the hiring of board members) or a vendor agreement (including contracting a cloud service provider) that gives a covered person access to bulk U.S. sensitive personal data is not ordinarily incident to and part of the provision of financial services for a financial institution's wholly domestic operations. Section 202.505 provides several additional examples as guidance. 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 may be separately exempt under § 202.507.

Issued on April 11, 2025.

Corporate-Group Transactions

76. Does the exemption for corporate-group transactions 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?

No. Section 202.506 exempts 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). While it is true that the administrative and ancillary business activities listed in the exemption are illustrative and not exhaustive, those exempt activities do not include research and development conducted by U.S. companies with corporate affiliates in countries of concern for the reasons explained in the final rule.

Issued on April 11, 2025.

Telecommunications Services

77. Does the telecommunications-services exemption include voice and data communications over the internet?

Yes. Under § 202.509, the telecommunications-services exemption applies to 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. Please note that the definition of telecommunications services in § 202.509 is limited to communications services and does not include all internet-based services like cloud computing.

Issued on April 11, 2025.

Compliance Requirements

78. How are U.S. companies, institutions, organizations, and individuals expected to comply with the DSP?

NSD expects that U.S. persons subject to the DSP will develop, implement, and update compliance programs as appropriate. Similar to economic sanctions, export controls, and other laws, 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. For guidance on compliance with the DSP, review the Cybersecurity and Infrastructure Security Agency (CISA) Security Requirements guidance and NSD's Compliance Guide.

Issued on April 11, 2025.

79. What are the "know your data" requirements?

The know-your-data requirements 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.

More generally, as part of a risk-based compliance program, NSD expects U.S. individuals and entities to take reasonable steps 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 awareness of the volume and types of data they possess and in which they are transacting.

Issued on April 11, 2025.

80. Do U.S. persons need to aggregate or decrypt their information to comply with "know your data" requirements?

No. Nothing in the DSP imposes a legal requirement to decrypt to comply. The NSD expects companies to know their data, but has been clear throughout the rulemaking process that decryption is not a required step in that effort.

Nothing in the DSP imposes a legal requirement to aggregate data to comply. Data-using entities typically maintain or have access to other 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. 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. For example, many 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.

For more information on why the DSP does not require decryption or aggregation to determine whether the bulk thresholds are satisfied, please see 89 Fed. Reg. 86127–86129.

Issued on April 11, 2025.

81. How do I verify the authenticity of an NSD specific license or advisory opinion?

If you have questions about the authenticity of an NSD-issued document that is not publicly posted on NSD's website, you may contact NSD at nsd.firs.datasecurity@usdoj.gov and refer to the specific document number or name appearing on the document.

Issued on April 11, 2025.

82. If I reject a prohibited transaction, when do I have to report the action to NSD? How do I submit the report?

Under § 202.1104, reports must be filed within 14 days of affirmatively rejecting a prohibited transaction involving data brokerage. U.S. persons must submit this report to NSD electronically by emailing nsd.firs.datasecurity@usdoj.gov or by using another official electronic reporting option in accordance with any instructions on NSD's website.

Issued on April 11, 2025.

83. Are U.S. persons expected to provide audit reports to NSD on an annual basis?

No. U.S. persons engaged in restricted transactions must retain the audit reports consistent with the recordkeeping requirements and must provide them to NSD only if requested. NSD may request, or use its subpoena power under § 202.1102 to compel, a company's audit reports and may use such audit reports as evidence, including in any enforcement action if the report demonstrates a company's failure to comply with the DSP. Any audit reports submitted to NSD would be subject to existing legal requirements regarding the protection of confidential or proprietary information.

Issued on April 11, 2025.

84. Can U.S. persons use audits completed for other purposes to comply with DSP?

Yes. The DSP requires that a company conduct an audit of its compliance with the DSP, but it does not require that a company conduct a separate audit to comply with the audit requirements. However, the audit must specifically, sufficiently, and expressly address the audit requirements set forth in the DSP.

Issued on April 11, 2025.

85. Can companies use internal auditors to audit compliance with the DSP?

Yes, so long as those internal audits are sufficiently independent. In NSD's 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, NSD 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. As a result, the DSP permits audits for restricted transactions to be either internal or external, so long as they are sufficiently independent and meet other requirements. NSD intends to provide additional guidance on the requirements for a sufficiently independent audit.

Issued on April 11, 2025.

86. Are the recordkeeping, reporting, or other requirements of the DSP a mechanism for the Federal Government to obtain access to the underlying data of U.S. persons?

No. Nothing in the DSP requires persons engaged in covered data transactions 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" without providing any of the underlying data. There may be limited circumstances in which NSD may need greater details about the underlying sensitive personal data, however, those limited circumstances should ordinarily be resolvable without needing access to the underlying data itself—such as through asking the parties questions about the nature of the data.

Issued on April 11, 2025.

87. Do the information reporting obligations in subpart K supersede Federal law that may otherwise restrict providing that information to governmental entities?

No. Subpart K imposes obligations on persons engaged in certain transactions subject to the DSP to report information about those transactions—including the parties to any such transactions—to the Department. *See*, 28 C.F.R. §§ 202.1102 (reports furnished on demand), 202.1103 (annual reports involving certain cloud-computing services), 202.1104 (reports on rejected prohibited transactions). Each of the reporting provisions includes an exception for reporting information that would otherwise be prohibited by Federal law. To that end, nothing in the DSP supersedes applicable Federal law (e.g., Stored Communications Act, 18 U.S.C. § 2701 *et seq.*). Persons subject to the recordkeeping and reporting obligations in subpart K are nonetheless required to maintain and report all information to the Department required by the DSP, consistent with Federal law and any lawfully authorized legal process, as necessary. NSD does not anticipate that the DSP recordkeeping and reporting provisions will conflict with other applicable Federal law. For example, nothing in the DSP requires parties engaged in covered data transactions to submit the underlying sensitive personal data to the Federal Government; see FAQ 86 for more information. Similarly, the DSP does not regulate, or require giving NSD access to, personal communications, expressive information, or informational materials; see FAQs 7, 71, and 72 for more information. However, persons subject to the reporting requirement or an NSD request for information should inform NSD in writing as part of making any required report or response to an NSD request, if they assess Federal law would otherwise prohibit providing NSD any information required in a report or response.

Issued on April 11, 2025.

88. Must all U.S. persons file annual reports of their compliance with the DSP?

No. 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.

Issued on April 11, 2025.

89. Does NSD require that U.S. persons set up a certain type of compliance program?

No, there is not a standard compliance program that would be sufficient or suitable for all U.S. persons and their data transactions. NSD will publish DSP Compliance Guide, which will provide additional information to assist in complying with the requirements for U.S. persons engaging in restricted transactions, including required aspects of a data compliance program, auditing, and recordkeeping. For more information on how to adhere to the Security Requirements issued by the Cybersecurity and Infrastructure Security Agency (CISA), see here.

Issued on April 11, 2025.

90. I am a U.S. person that engages in restricted transactions. What does my due diligence process need to consist of to meet the requirements of the DSP?

What constitutes an adequate compliance program depends in large part on what kind of business you do, where you operate, and with whom. Certain types of bulk U.S. personal sensitive data or government related data may pose a higher risk to U.S. national security than others. The DSP does not prescribe or endorse any specific method to screen counterparties to determine their status as covered persons. Consistent with the DSP, 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. For guidance on compliance measures that are required for engaging in restricted transactions, please review the Cybersecurity and Infrastructure Security Agency (CISA) Security Requirements guidance and NSD's Compliance Guide.

Beginning on October 6, 2025, U.S. persons engaged in restricted transactions must comply with additional due-diligence, auditing, and reporting requirements.

Issued on April 11, 2025.

91. How often do I need to screen my vendor, employee, and investor databases against the Covered Persons List to see if I am engaging in data transactions with covered persons?

The frequency of screening transaction parties against the Covered Persons List must be guided by your organization's internal policies and procedures, based on your individualized risk profile. Keep in mind, however, that the Covered Persons List is not exhaustive, and some foreign persons are covered persons based on ownership, employment, or residence.

Issued on April 11, 2025.

92. What documents do U.S. persons need to retain to comply with §§ 202.1002 and 202.1101?

Under § 202.1002(b)(3), U.S. persons engaged in restricted transactions must retain audit reports for a period of at least 10 years, consistent with the recordkeeping requirements in § 202.1101. Under § 202.1101, U.S. persons engaging in any transaction subject to the provisions of the DSP must 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. Section 202.1101(b) lists the baseline for records that must be maintained by a U.S. person engaging in any restricted transaction. The DSP provides the minimum obligations for recordkeeping. U.S. persons must develop retention policies and procedures that are, at minimum, consistent with the DSP, and based on the company's 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.

Please also note that the recordkeeping requirements do not apply to exempt transactions except to the extent required as a condition of a specific exemption. See FAQ 70 for more information.

Issued on April 11, 2025.

93. What criteria will NSD consider in evaluating whether an internal auditor is "independent" for purposes of § 202.1002?

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. As such, the DSP does not prohibit U.S. persons from conducting internal audits to satisfy the requirements of § 202.1002.

Criteria relevant to establish "independence" may vary based on a range of factors, including the U.S. person's internal corporate structure, the internal auditor's accountability to senior leadership and/or the U.S. company's board of directors, as well as the training and expertise possessed by the internal auditor. Appropriate safeguards may also implicate the complexity of the auditing process, the U.S. company's size and sophistication, products and services, customers and counterparties, and geographic locations, as well as the sensitivity and volume of covered transactions at issue.

For more guidance on audit requirements, see the Data Security Program: Compliance Guide.

Issued on April 11, 2025.

Licensing

94. Can I appeal a denial of my license application?

NSD's denial of a license application constitutes final agency action. The DSP does not provide for a formal process of appeal. However, NSD will reconsider its determinations for good cause,

for example, where the applicant can demonstrate changed circumstances or submit additional relevant information not previously made available to NSD.

Issued on April 11, 2025.

95. What are the chances my license application will be approved?

NSD's primary mission with respect to the implementation and enforcement of Executive Order 14117, and the DSP (28 C.F.R. part 202) is protecting Americans from countries that may seek to collect and weaponize Americans' most sensitive data. To address the unusual and extraordinary threat to the national security and foreign policy of the United States posed by the continuing efforts of countries of concern to access Americans' bulk sensitive personal data and U.S. Government-related data, and given that the DSP's prohibitions and restrictions are closely tailored to this risk, NSD will apply a "presumption of denial" standard for all license applications. Each application will be reviewed on a case-by-case basis. Ordinarily, to overcome this presumption, a license application will need to affirmatively identify compelling countervailing considerations to support the issuance of a specific license (such as an emergency or imminent threat to public safety or national security). Parties should consider whether such considerations are present before applying for a license. NSD 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. *See* § 202.803(d).

Issued on April 11, 2025.

96. Can I submit a specific licensing application to request that NSD issue a general license?

No. Companies seeking licenses should submit requests for specific licenses, not general licenses. NSD 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 NSD otherwise learns of a need to issue a general license, such as via industry engagement.

Issued on April 11, 2025.

97. When can I submit my specific license application?

NSD will target its enforcement efforts during the first 90 days to allow U.S. persons (*e.g.*, individuals and companies) additional time to implement the changes required by the DSP, provide additional opportunities for the public to engage with NSD on DSP-related inquiries, and to minimize potential disruptions for businesses.

Specifically, NSD will not prioritize civil enforcement actions against any person for violations of the DSP that occur from April 8 through July 8, 2025, so long as the person is engaging in good faith efforts to comply with or come into compliance with the DSP during that time. These efforts include engaging in activities enumerated in NSD's Data Security Implementation and Enforcement Policy Through July 8, 2025, including amending or renegotiating existing contracts, conducting internal reviews of data flows, deploying the CISA security measures, etc. *See also* FAQ 4.

This policy does not limit NSD's lawful authority and discretion to pursue civil enforcement if such persons did not engage in good faith efforts to comply with, or come into compliance with, the DSP.

During this 90-day period, NSD encourages the public to contact NSD at nsd.firs.datasecurity@usdoj.gov with informal inquires or information about the DSP and the guidance NSD has released. Although NSD may not be able to respond to every inquiry, NSD will use its best efforts to respond consistent with available resources, and any inquiries or information submitted may be used to develop and refine future guidance. Correspondingly, NSD discourages the submission of any formal requests for specific licenses during this 90-day period: Although requests for specific licenses during this 90-day period can be submitted, NSD will not review or adjudicate those submissions during the 90-day period (absent an emergency or imminent threat to public safety or national security).

Issued on April 11, 2025.

Advisory Opinions

98. Can I apply advisory opinions that NSD issued to other parties as guidance for my prospective transactions?

Under § 202.901(i), each advisory opinion can be formally relied upon only "by the requesting party or parties" (not third parties) to the extent the disclosures made pursuant to § 202.901 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.

That said, NSD may, at its discretion and following discussions with the original requester, publish certain advisory opinions, and other parties may find these advisory opinions useful. In relying on these advisory opinions, however, other parties should take great care to ensure that the transactions in question fully conform to the letter and spirit of the published materials, that the relevant facts and circumstances are materially similar, and that the materials have not been superseded. NSD encourages U.S. persons to file their own request for an advisory opinion where that U.S. person is concerned about whether the scenario in a published advisory opinion is applicable.

NSD 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 NSD action in response to any advisory opinion request, consistent with applicable law, and to use any such request, document, or information for any governmental purpose.

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 NSD will consider a party's reliance on the superseded advisory opinion to be unreasonable, and any transition period that may be applicable.

Issued on April 11, 2025.

99. Can NSD change its previously published advisory opinion without first giving public notice?

Yes. An advisory opinion may be amended or revoked at any time after it has been issued based on a change in NSD's understanding of the facts. Subsequent notice of such will be given in the same manner as notice of the advisory opinion was originally given or in the Federal Register. NSD therefore strongly encourages parties to exercise due diligence when their business activities may touch on the DSP and to contact NSD at nsd.firs.datasecurity@usdoj.gov if they have any questions about their transactions.

Issued on April 11, 2025.

100. Can foreign persons (whether covered persons or not) seek advisory opinions on behalf of a U.S. person with whom the foreign person is a counterparty for an in-process or contemplated covered data transaction?

Generally, no. The decision to seek an advisory opinion from NSD about a specific, non-hypothetical transaction is entirely voluntary, and only U.S. persons who are parties to a transaction that the DSP potentially regulates, or an agent of that U.S. person-party, may seek an advisory opinion from NSD.

Issued on April 11, 2025.

101. When can I send in an advisory opinion request?

NSD will target its enforcement efforts during the first 90 days to allow U.S. persons (*e.g.*, individuals and companies) additional time to implement the changes required by the DSP, provide additional opportunities for the public to engage with NSD on DSP-related inquiries, and to minimize potential disruptions for businesses.

Specifically, NSD will not prioritize civil enforcement actions against any person for violations of the DSP that occur from April 8 through July 8, 2025, so long as the person is engaging in good faith efforts to comply with or come into compliance with the DSP during that time. These efforts include engaging in activities enumerated in NSD's Data Security Program Implementation and Enforcement Policy Through July 8, 2025, including amending or renegotiating existing contracts, conducting internal reviews of data flows, deploying the CISA security measures, etc. *See also* FAQ 4.

This policy does not limit NSD's lawful authority and discretion to pursue civil enforcement if such persons did not engage in good faith efforts to comply with, or come into compliance with, the DSP.

During this 90-day period, NSD encourages the public to contact NSD at nsd.firs.datasecurity@usdoj.gov with informal inquires or information about the DSP and the guidance NSD has released. Although NSD may not be able to respond to every inquiry, NSD will use its best efforts to respond consistent with available resources, and any inquiries or information submitted may be used to develop and refine future guidance. Correspondingly, NSD discourages the submission of any formal requests for advisory opinions during this 90-day period: Although requests for advisory opinions during this 90-day period can be submitted, NSD will not review or adjudicate those submissions during the 90-day period (absent an emergency or imminent threat to public safety or national security).

Issued on April 11, 2025.

Enforcement Guidance

102. How much are the penalties for violating the DSP?

Violations of the DSP may result in civil and, in some cases, criminal penalties, which can be substantial. The legal basis for the DSP is the International Emergency Economic Powers Act (IEEPA), which 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. NSD will make annual adjustments to the maximum civil penalty amount consistent with the Federal Civil Penalties Inflation Adjustment Act. 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 may, upon conviction, be fined not more than $1,000,000, or if a natural person, be imprisoned for not more than 20 years, or both.

Issued on April 11, 2025.

103. Will NSD impose strict liability for violations of the DSP?

No. While IEEPA authorizes strict liability for violations and other IEEPA-based programs, (such as sanctions administered by the Department of the Treasury's Office of Foreign Assets Control), the DSP's prohibitions include a knowledge standard.

Issued on April 11, 2025.

104. Can NSD demand, in the form of reports or otherwise, 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?

Yes, see § 202.1102. IEEPA and E.O. 14117 authorize comprehensive implementing and penalties provisions that enable NSD, among other things, to promulgate regulations and issue administrative subpoenas, licenses, and the full range of civil enforcement actions with respect to DSP violations. NSD 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. NSD 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.

Issued on April 11, 2025.

105. How can I self-disclose a possible violation of the DSP?

NSD may consider a qualifying voluntary self-disclosure as a mitigating factor in any enforcement action, which may result in a reduction in the base amount of any proposed civil penalty. Please submit all voluntary self-disclosures electronically to nsd.firs.datasecurity@usdoj.gov with "Voluntary Self-Disclosure" in the subject. In addition to notifying NSD of an apparent violation, a voluntary self-disclosure must include, or be followed within a reasonable period of time by, a report of sufficient detail to afford NSD a complete understanding of an apparent violation's circumstances. When such a report is not included with an initial notification, NSD will generally expect such a report within 180 days after the initial notification.

Issued on April 11, 2025.

106. How can I report a possible violation of the DSP by another person?

Individuals reporting violations of the DSP may be eligible for financial incentives if they do so through FinCEN's whistleblower incentive program. FinCEN maintains a whistleblower program for violations of several specific statutes enforced by Justice or Treasury, including the IEEPA, which the DSP falls under. Individuals located in the United States or abroad who provide information about violations of the DSP may be eligible for substantial financial awards, if the information they provide leads to a successful enforcement action by NSD that results in monetary penalties exceeding $1,000,000. Individuals can learn more about FinCEN's whistleblower program, including how to submit a tip or report, by contacting FinCEN.

Issued on April 11, 2025.

107. Will NSD impose a penalty if my apparent violation of the DSP was inadvertent?

It depends. The DSP prohibits U.S. persons from knowingly engaging in certain covered data transactions, like transactions involving data brokerage or bulk human 'omic data, and from knowingly engaging in other covered data transactions, like vendor, employment, and investment agreements, unless they comply with the security requirements imposed by § 202.408. This knowledge standard means, 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, NSD will take into account the relevant facts and circumstances, including the relative sophistication of the individual or entity at issue, the scale and sensitivity of the data involved, and the extent to which the parties to the transaction at issue appear to have been aware of and sought to evade the application of the DSP. As a result of this knowledge standard, the DSP's incorporation of the word "knowingly" does not adopt a strict liability standard. NSD will review the totality of the circumstances surrounding any apparent violation, including whether a matter was voluntarily self-disclosed to NSD. Such disclosure may also support credit for cooperation. NSD's forthcoming enforcement guidance will provide additional information regarding voluntary self-disclosures and other mitigating factors, as well as NSD's general framework for the enforcement of the DSP.

Issued on April 11, 2025.

108. I am a U.S. person that is subject to an NSD enforcement investigation for engaging in a covered data transaction with a designated covered person in violation of the DSP. Since the initiation of this investigation, NSD delisted and removed the Covered Person from the Covered Persons List. Will the enforcement investigation cease now that the designation has been removed?

The revocation of a designation does not affect past, present, or future NSD enforcement investigations or actions associated with any apparent violations of the DSP that occurred before the revocation. Pending NSD enforcement matters may proceed irrespective of the termination of NSD-administered designations, and NSD may continue to review apparent violations of the DSP, whether they came to the agency's attention before or after the designation was revoked. An apparent DSP violation is analyzed using the laws and regulations, including designations of covered persons, that were in place at the time of the underlying activities that form the basis for the apparent violation, and civil and criminal enforcement authorities are applied accordingly. Current or future investigations regarding apparent violations of the DSP may not be impacted by the subsequent revocation of a designation and may result in NSD enforcement actions.

Issued on April 11, 2025.