Department of Justice

April 11, 2025
www.justice.gov

National Security Division
Foreign Investment Review Section

DATA SECURITY PROGRAM: COMPLIANCE GUIDE

I. Introduction

The Data Security Program ("DSP") implemented by the National Security Division ("NSD") under Executive Order 14117[1] ("the Order") comprehensively and proactively addresses the continued efforts of foreign adversaries to use commercial activities to access, exploit, and weaponize U.S. Government-related ("government-related") data and Americans' bulk sensitive personal data.

The Order, among other things, directed the U.S. Department of Justice (the "Department") to issue regulations that prohibit or otherwise restrict United States persons from engaging in certain transactions. On January 8, 2025, the Department's National Security Division ("NSD") published a final rule implementing the Order, codified at 28 CFR Part 202 ("Data Security Program" or "DSP").[2] The DSP addresses this "unusual and extraordinary threat… to the national security and foreign policy of the United States" that has been repeatedly recognized across political parties and by all three branches of Government—including, notably, in the 2025 Annual Threat Assessment of the U.S. Intelligence Community and the President's America First Investment Policy, NSPM-2 on Imposing Maximum Pressure on Iran, national emergency declared in Executive Order 13873,[3] and 2017 National Security Strategy. To address this urgent threat, the DSP establishes what are effectively export controls that prevent foreign adversaries, and those subject to their control and direction, from accessing U.S. Government-related data and bulk U.S. sensitive personal data.

NSD's primary mission with respect to the implementation and enforcement of the Data Security Program is to protect U.S. national security from countries of concern that may seek to collect and weaponize Americans' most sensitive personal data. U.S. persons must comply with the Data Security Program. Any individual or entity who conspires or seeks to evade the DSP's restrictions or prohibitions can potentially be subject to criminal or civil penalties. U.S. persons should "know their data," including the kinds and volumes of data collected about or maintained on U.S. persons or U.S. devices; how their company uses the data; whether their company engages in covered data transactions; and how such data is marketed, particularly with respect to

[1] Executive Order 14117 of February 28, 2024 (Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern).
[2] Unless otherwise indicated, all citations are to the sections of the DSP regulations in 28 CFR part 202.
[3] Executive Order 13873 of May 15, 2019 (Securing the Information and Communications Technology and Services Supply Chain).

current or recent former employees or contractors, or former senior officials, of the United States government, including the military and Intelligence Community.

This document is 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. This document is explanatory and intended to provide general guidance to regulated parties seeking to comply with the DSP. This document does 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. Persons seeking to comply with the legally binding provisions in the DSP should refer to 28 CFR part 202. This document does not alter those legal requirements. To the extent that there is any apparent inconsistency between this Compliance Guide and IEEPA, Executive Order 14117, or the implementing regulations, the latter control. Compliance with the guidance in this document shall not be deemed to satisfy the DSP and shall not be a defense to enforcement actions brought for violations or suspected violations of the DSP. Conversely, failing to adhere to this guidance shall not be deemed to violate the DSP, unless a party violates the legally binding provisions of the DSP itself.

II. Background

A. Effective Date

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.

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. Please see NSD's Data Security Program: Implementation and Enforcement Policy Through July 8, 2025 for more information.

B. Countries of Concern

The Department has designated the following countries as a country of concern:

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

These countries of concern demonstrate an intent and capability to use U.S. Government-related data and Americans' sensitive personal data to threaten U.S. national security, including espionage and economic espionage, surveillance, coercion and influence, blackmail, foreign malign influence, curbing dissent by U.S. persons, targeting journalists, political figures, members of marginalized communities, and other populations, and engaging in nefarious, cyber-enabled activities.

C. Covered Data Transactions

A covered data transaction is any transaction that involves any access by a country of concern or covered person to any government-related data or bulk U.S. sensitive personal data and that involves: (1) data brokerage;[4] (2) a vendor agreement;[5] (3) an employment agreement;[6] or (4) an investment agreement.[7]

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. Examples of such locations can be found at § 202.222(a)(1). 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 two years of a potential covered data transaction with a country of concern or covered person.

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 bulk threshold set forth in § 202.205. The term "sensitive personal data" means covered personal identifiers, precise geolocation data, biometric identifiers, human 'omic data, personal health data, personal financial data, or any combination thereof.[8] Sensitive personal data 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. Even anonymized data, when aggregated, can still be used by countries of concern

[4] § 202.214.
[5] § 202.258.
[6] § 202.217.
[7] § 202.228.
[8] *See* § 202.249 for applicable exclusions.

and covered persons to identify individuals and to conduct malicious activities that implicate the risk to national security the Order was intended to address.

D. Covered Persons

The Order directed the Department to identify, with the concurrence of the Secretaries of State and Commerce, classes of covered persons.[9] A covered person is an individual or entity that, whether or not publicly designated by the Department, falls into one of the classes of covered persons described in the DSP; or is any individual or entity that the Department has designated and publicly determined to be a covered person. A U.S. person is never a covered person unless designated as such by the Department under § 202.211(a)(5). The five categories of covered persons are defined in § 202.211(a).

The four classes of persons that are covered persons whether or not designated are: (1) foreign entities headquartered in or organized under the laws of a country of concern or 50% or more owned, individually or in the aggregate, by one or more countries of concern or other covered persons; (2) foreign entities 50% or more owned, individually or in the aggregate, by a country of concern or another covered person; (3) foreign individuals that are employees or contractors of a country of concern or covered person; and (4) foreign individuals who are primarily resident in a country of concern. Covered persons falling into the above categories of § 202.211(a)(1)-(4) do not require identification or designation by NSD. These persons' status as a covered person is based on meeting the defined criteria in the DSP at the time of the covered data transaction.

The fifth category of covered persons is those persons NSD designates and publicly identifies, pursuant to § 202.211(a)(5). NSD has the authority to designate both foreign and U.S. persons as covered persons pursuant to § 202.211(a)(5), after a determination that those persons meet certain criteria, such as being subject to the ownership or control of a country of concern. NSD will add designated covered persons to the Covered Persons List and will publish notices in the Federal Register identifying such persons as covered persons. Designated covered persons retain their covered persons status, even when located in the United States.

III. Prohibited Transactions

Under § 202.243, the term "prohibited transaction" means a data transaction that is subject to one or more of the prohibitions described in DSP subpart C. The prohibited transactions described in §§ 202.301 – 202.302 involve covered data transactions that involve data brokerage. The prohibitions involving data brokerage in subpart C apply to the sale or licensing of access to data, or similar commercial transactions, involving the transfer of data from any person (the provider) to any other person (the recipient), where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data. Accordingly, the prohibitions involving data brokerage in subpart C would prohibit first-party (or primary) data brokers, who collect and sell information from their own customers, and third-party data brokers, who purchase and resell data that they did not collect in the first instance, from engaging in data brokerage transactions involving bulk U.S. sensitive personal data or government-related data with (1) countries of concern or covered persons[10] or

[9] § 202.211(a).
[10] § 202.301.

(2) other foreign persons, unless the data brokerage transaction included a contractual prohibition on resale of any such data.[11] Section 202.303 prohibits any data transactions with countries of concern or covered persons involving access to bulk human 'omic data. Section 202.304 covers prohibited evasions, attempts, the causing of violations, and conspiracies. Section 202.305 prohibits knowingly directing prohibited or restricted transactions.

A. Prohibited Transactions with Countries of Concern or Covered Persons

Under § 202.301, unless exempt or otherwise authorized by a general or specific license, U.S. persons may not knowingly engage in a covered data transaction involving data brokerage with a country of concern or covered person. Under § 202.214, 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. To determine what an individual or entity reasonably should have known in the context of prohibited transactions, NSD may take into account all relevant facts and circumstances, including the relative sophistication of the individual or entity at issue.

Given the data brokerage definition, U.S. persons should seek to understand whether their activities would be prohibited by the DSP because they would enable covered persons or countries of concern to access government-related or bulk U.S. sensitive personal data. Some activities that may not be thought of in ordinary parlance as data brokerage may nonetheless constitute data brokerage under the DSP, such as a U.S. company maintaining a website or mobile application that contains ads with tracking pixels or software development kits that were knowingly installed or approved for incorporation into the app or website by the U.S. company. That transfer or provision of access to government-related or bulk U.S. sensitive personal data to covered persons or countries of concern could constitute data brokerage and could be a violation of the DSP.

B. Prohibited Transactions with Foreign Persons

The DSP also contains prohibitions for covered data transactions involving data brokerage with foreign persons that are not covered persons.[12] Under § 202.302, unless exempt or otherwise authorized by a general or specific license, U.S. persons may not knowingly engage in a data transaction involving data brokerage with a foreign person unless the U.S. person (1) contractually requires that the foreign person refrain from engaging in a subsequent covered data transaction involving data brokerage of the same data with a country of concern or covered person; and (2) reports any known or suspected violations of this contractual requirement in accordance with § 202.302(b).

1. Contractual Language

U.S. persons engaging in data transactions involving data brokerage with foreign persons (who are not covered persons) must include contractual language prohibiting the foreign person

[11] § 202.302.

[12] Generally, when engaging in covered data transactions with a foreign person that is an entity, U.S. persons are not expected to conduct due diligence on the employment practices of those foreign persons to determine whether the foreign person's employees qualify as covered persons.

from engaging in the onward transfer or resale of government-related data or bulk U.S. sensitive personal data to countries of concern or covered persons.[13]

No particular form or specific contractual language is required by the DSP to prohibit onward sale or transfer. Parties may wish to tailor their contractual language based on several factors, including the relevant business activity, risk appetite, the contract counterparties, the products and services involved, and the bulk U.S. personal sensitive or government-related data at issue.

As an example, U.S. persons may consider including some variation of the following language, signed by authorized representatives of the U.S. person and the foreign person counterparty:

> *[U.S. person] provides [foreign person] with a non-transferable, revocable license to access the [data subject to the brokerage contract]. [Foreign person] is prohibited from engaging or attempting to engage in, or permitting others to engage or attempt to engage in the following:*
>
> *(a) selling, licensing of access to, or other similar commercial transactions, [such as reselling, sub-licensing, leasing, or transferring in return for valuable consideration,] the [data subject to the brokerage contract] or any part thereof, to countries of concern or covered persons, as defined in 28 CFR part 202;*
>
> *Where [foreign person] knows or suspects that a country of concern or covered person has gained access to [data subject to the brokerage contract] through a data brokerage transaction, [foreign person] will immediately inform [U.S. person]. Failure to comply with the above will constitute a breach of [data brokerage contract] and may constitute a violation of 28 CFR part 202.*

This language is just an example. U.S. persons should craft language that satisfies the DSP's requirements and that makes sense for their transactions and business operations.

U.S. persons may also wish to include in their contracts language that requires foreign persons to periodically certify their compliance with this contractual restriction on onward transfer and to obligate the foreign person not to evade or avoid, cause a violation of, or attempt to violate any of the prohibitions set forth in Executive Order 14117 or 28 CFR part 202. As an example, U.S. persons could include language in their contracts like the following:

[Foreign person] confirms that for [the brokerage contract], [foreign person] is in compliance with 28 CFR part 202 and any other prohibitions, restrictions or provisions applicable to the [data subject to the brokerage contract]. [Foreign person] agrees to [periodically] certify to [U.S. person], in writing [foreign person's] compliance with 28 CFR part 202. [Foreign person] agrees to not evade or avoid, cause a violation of, or attempt to violate any of the prohibitions set forth in Executive Order 14117 or 28 CFR part 202]

[13] As a reminder, under § 202.301, unless exempt or otherwise authorized, it is prohibited for a U.S. person to engage in covered data transactions involving data brokerage with covered persons or countries of concern. Inclusion of contractual language regarding use or onward sale of the data will not authorize a U.S. person to engage in such a transaction with a covered person or country of concern.

Notwithstanding the use of any such clauses, U.S. persons subject to the DSP must still maintain appropriate systems and controls, including reasonable and proportionate due diligence, to mitigate the risk they breach the DSP. U.S. persons engaged in these kinds of data brokerage transactions with non-covered foreign persons and third countries should not simply shift responsibility to or entirely rely on the contractual provisions or on their foreign counterparties to comply with these contractual provisions. Instead, as the Notice of Proposed Rulemaking explains, consistent with the overall approach to compliance and enforcement under the DSP, NSD expects U.S. persons engaged in these kinds of data brokerage transactions to take reasonable steps to evaluate whether their foreign counterparties are complying with the contractual provision as part of implementing risk-based compliance programs under the proposed rule. NSD will review the totality of the circumstances surrounding covered data transactions, including the parties involved therein and contractual language adopted to satisfy § 202.302 when determining whether a party has complied with the DSP's requirements and prohibitions. Generally, absent indications of evasion, conspiracy, or knowingly directing prohibited transactions, U.S. persons that conduct adequate due diligence as part of a risk-based compliance program would not have engaged in a prohibited transaction if the foreign counterparty later violates the required contractual provision or if the U.S. person fails to detect such violations. Depending on the circumstances, a U.S. person's failure to conduct adequate due diligence may subject the U.S. person to enforcement actions if that failure would constitute an evasion of the regulations, such as repeatedly knowing of violations by a foreign person and continuing to engage in data-brokerage transactions with that foreign person.

2. Reporting Known or Suspected Violations

The transactions involving data brokerage described in § 202.302 are prohibited unless, among other things, the U.S. person party to the transaction reports known or suspected violations of the contractual requirements described in § 202.302(a)(1). U.S. persons must report any known or suspected violation of contractual requirements required under § 202.302(a)(1) within 14 days of suspecting a violation or becoming aware of a violation.
Section 202.302(b)(2) lists the required contents of this report. Reports must include all information required by the DSP that are readily available to the person providing the report at the time the report is made. NSD generally does not expect those persons to seek further information from parties to the transaction solely to obtain additional information required under § 202.302(b)(2). As a best practice, reports should include information that is applicable in all reported violation scenarios (e.g., information regarding the submitter of the report, the legal authority or authorities under which the transaction is being reported, and the date of the known or suspected violation or the date of discovery). The required report must be submitted in accordance with § 202.302(b) and subpart L. Whether such a § 202.302(b)(2) report would constitute a Voluntary Self-Disclosure (VSD) is a fact-specific inquiry. NSD may separately issue DSP Enforcement Guidance to provide additional information on VSDs. U.S. companies must retain relevant records for ten years, in accordance with the requirements of subpart K.

U.S. persons must exercise due diligence to ensure and monitor compliance with such contractual provisions prohibiting potential onward transfer to countries of concern or covered persons. The DSP requires U.S. persons to reject participating in any transaction that violates the DSP, and to report such a rejected transaction to NSD, in accordance with § 202.1104, as further discussed in Part III(F)(2) of this Compliance Guide.

C. Prohibited Transactions Involving Human 'Omic Data or Related Human Biospecimens

Under § 202.303, unless exempt or otherwise authorized by a general or specific license, U.S. persons may not knowingly engage 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. Human 'omic data includes human genomic, epigenomic, proteomic, and transcriptomic data, but excludes pathogen-specific data embedded in human 'omic data sets. The term human biospecimens means a quantity of tissue, blood, urine, or other human-derived material, including such material classified under any of the 10-digit Harmonized System-based Schedule B numbers listed in § 202.223. The term human biospecimens excludes any human biospecimens, including human blood, cell, and plasma-derived therapeutics, intended by a recipient solely for use in diagnosing, treating, or preventing any disease or medical condition.

The DSP exempts certain covered data transactions that may be relevant to U.S. persons engaging in data transactions involving human 'omic data, including for example, covered data transactions that are conducted pursuant to a grant, contract, or other agreement with Federal departments and agencies; covered data transactions ordinarily incident to clinical investigations and post-marketing surveillance; covered data transactions that are required or authorized by certain specified international arrangements addressing global and pandemic preparedness. For more information on these and other exempt transactions, see subpart E.

D. Prohibited Evasions, Attempts, Causing Violations, and Conspiracies

Section 202.304 prohibits any transaction that has the purpose of evading or avoiding, causes a violation of, or attempts to violate any of the prohibitions set forth in the DSP. This provision also prohibits any conspiracy to violate the prohibitions in the DSP. NSD is authorized to bring enforcement actions and criminal prosecutions pursuant to the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. §§ 1701 *et seq.*, the underlying authority for the Order and DSP, for knowing violations of the Data Security Program. Unlawful acts under IEEPA are subject to civil penalties of up to the greater of $368,136 or twice the value of each violative transaction. Willful violations of IEEPA are punishable by imprisonment of up to 20 years and a $1,000,000 fine. NSD may separately issue DSP Enforcement Guidance to provide more information on violations of the DSP, including what NSD will consider a "transaction" for the purpose of calculating penalties.

E. Knowingly Directing Prohibited Transactions

Unless exempted or authorized by a general or specific license, knowingly directing a prohibited covered data transaction or restricted transaction without meeting additional applicable requirements could constitute a violation of the DSP.[14] Under § 202.230(a), the term knowingly, with respect to conduct, a circumstance, or a result, means that a person has actual knowledge, or reasonably should have known, of the conduct, the circumstance, or the result. Under § 202.215, a person directs an action if the person has any authority (individually or as

[14] § 202.305(a).

part of a group) to make decisions for or on behalf of an entity and exercises that authority to effectuate the action.

As noted above, U.S. persons engaging in vendor agreements and other classes of data transactions with foreign persons are generally not expected to conduct due diligence on the employment practices of those foreign persons to determine whether their employees qualify as covered persons. Generally, a U.S. person has not knowingly directed a restricted transaction where that U.S. person engages in a vendor agreement involving bulk U.S. sensitive personal data with a foreign person who is not a covered person and that foreign person, in turn, employs an individual who is a covered person and grants them access to bulk U.S. sensitive personal data without the U.S. person's knowledge or direction. It may, however, constitute a DSP violation for that U.S. person to knowingly direct that foreign person company to enter an employment agreement with that covered person to indirectly accomplish what would otherwise be a prohibited or restricted transaction if engaged in directly by the U.S. person.[15]

F. Recordkeeping and Reporting Requirements

1. Recordkeeping Requirements

The DSP recordkeeping requirements are contained in § 202.1101. Except as otherwise provided, U.S. persons engaging in any transaction subject to the DSP must keep a full and accurate record of each such transaction engaged in, and such record must be available for examination for at least ten years after the date of such transaction. Section 202.1101(b) lists the records that U.S. persons are obligated to create and maintain in an auditable manner.

U.S. persons should familiarize themselves with when the recordkeeping requirements of § 202.1101 apply. First, the recordkeeping requirements apply to any non-exempt covered data transaction. Second, the recordkeeping requirements apply to covered data transactions authorized by a general or specific license. In some instances, general and specific licenses may impose additional or different recordkeeping requirements. Third, the recordkeeping requirements set forth in §§ 202.1101(a) apply to covered data transactions conducted under the exemption in § 202.510 concerning certain drug, biological product, and medical device authorizations.

Of note, the recordkeeping requirements do <u>not</u> apply to any covered data transaction conducted under the following exemptions: the official business of the United States Government, § 202.504; financial services, § 202.505; corporate group transactions, § 202.506; transactions required or authorized by Federal law or international agreements, or necessary to comply with Federal law, § 202.507; investment agreements subject to a CFIUS action, § 202.508; telecommunications services, § 202.509; and clinical investigations and post-marketing surveillance data, § 202.511.

2. Reporting Requirements

The DSP also imposes certain reporting requirements, set out in §§ 1102, 1103, and 1104. Section 202.1102 requires every person to furnish under oath, in the form of reports or otherwise, from time to time and at any time as may be required by NSD, complete information

[15] § 202.305(b)(8).

relative to any act or covered data transaction, regardless of whether such act or covered data transaction is affected pursuant to license or otherwise, subject to the provisions of subpart K.

Section 202.1103 describes annual reporting obligations for persons engaged in certain restricted transactions. This is further discussed in Part IV(E) below.

Section 202.1104 concerns reporting rejected prohibited transactions involving data brokerage. U.S. persons must not participate in a prohibited transaction involving data brokerage that violates the DSP. In accordance with § 202.1104, U.S. persons that affirmatively reject engaging in such conduct (including where participation is automatically rejected using software, technology, or automated tools) are required to report the transaction to NSD within 14 days of the rejection. Section 202.1104(c) lists the required contents of this report. Reports must provide all information required by the DSP that are in the reporting person's possession. NSD generally does not expect those persons to seek further information from parties to the transaction solely to obtain additional information required under § 202.1104(c). Reports must, at a minimum, include required information that is applicable in all scenarios (e.g., information regarding the submitter of the report, the date the transaction was rejected, the counterparty proposing the transaction, the types and volumes of government-related data or bulk U.S. sensitive personal data the counterparty sought, the legal authority or authorities under which the transaction was rejected, and any relevant documentation received in connection with the transaction). The required report must be submitted in accordance with subpart L. Whether such a report would constitute a Voluntary Self-Disclosure (VSD) is a fact specific inquiry. NSD may separately issue DSP Enforcement Guidance to provide additional information on VSDs.

IV. Restricted Transactions[16]

Under §§ 202.246 and 202.401, unless exempt or otherwise authorized by a general or specific license, U.S. persons may not knowingly engage 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"[17]), unless the U.S. person complies with all applicable Data Security Program requirements, including the security requirements imposed by subpart D. Specifically, U.S. persons engaging in any restricted transactions must comply with: (1) the security requirements, as incorporated by reference in § 202.248; (2) all Data Compliance Program development and implementation requirements under § 202.1001; (3) the obligation to

[16] Please note that Section IV(A)'s discussion of CISA security requirements and other compliance requirements is applicable only for U.S. persons engaging in *restricted transactions* and is not applicable to *prohibited transactions*. Stated more specifically, a U.S. person's development and implementation of a compliance program would **not** authorize that U.S. person to engage in prohibited transactions.

[17] Please note that 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 28 CFR § 202.303. Also note that it is not a restricted transaction to engage in a covered data transaction involving a vendor, employment, or investment agreement with a foreign person who is not a covered person.

conduct audits that comply with the requirements of § 202.1002; and (4) the recordkeeping requirements under §§ 202.1101–1104.

A. Security Requirements

The Cybersecurity and Infrastructure Agency (CISA) Security Requirements for restricted transactions are incorporated by reference into the DSP. *See* §§ 202.248, 202.401(b). For more information, see the CISA Security Requirements.

B. Data Compliance Program

Under § 202.246 and subpart J, the DSP imposes an affirmative due diligence requirement on all U.S. persons engaged in restricted transactions to develop, implement, and routinely update an individualized, risk-based, written Data Compliance Program. This program should be designed to prevent, detect, and remediate breaches in company procedures and violations of the DSP. The failure to adopt and maintain adequate data compliance policies and procedures is potentially a violation of the DSP and may be an aggravating factor in any enforcement action. Although a U.S. person's Data Compliance Program should, as a best practice, be tailored to the U.S. person's risk profile, it must meet several minimum requirements to comply with the DSP. Below is guidance to help individuals and entities design and implement a Data Compliance Program that meets these minimum affirmative requirements in the DSP, as well as broader suggestions about how to design and implement a more robust Data Compliance Program. Whether a Data Compliance Program complies with the DSP's requirements is a holistic inquiry that depends on the facts and circumstances. Compliance with the suggestions outlined below may not satisfy the DSP's requirements in all circumstances and will not provide a safe harbor for apparent violations of the DSP. Conversely, failing to adopt the suggestions described below may not violate the DSP.

1. Due Diligence

i. Risk-Based Procedures

First, under § 202.1001(b)(1), a U.S. person's Data Compliance Program must establish and implement risk-based procedures for verifying data flows involved in any restricted transaction, including procedures to verify and log, in an auditable manner, the following: (1) the types and volumes of bulk U.S. sensitive personal data or government-related data involved in any restricted transactions; (2) the identity of the transaction parties, including any ownership of entities or citizenship or primary residence of individuals; and (3) the end-use of the data and the method of data transfer.

A company's risk profile may vary depending on a range of factors, such as the company's size and sophistication, products and services, customers and counterparties, and geographic locations. As a best practice for designing a robust Data Compliance Program, U.S. persons could conduct routine (ideally, at least annual) and ongoing risk assessments to evaluate the potential issues they are likely to encounter based on their business activity and risk appetite. Such a risk assessment could assess coverage of the regulations against the company's current data holdings and vendor, employee, or investment agreements. Companies may wish to review these risk assessments in the context of mergers and acquisitions, divestments, spin-offs, or other corporate transactions. Personnel could update risk assessments following apparent violations or

systemic deficiencies uncovered as the result of an audit or breach, or as identified by the organization during the routine course of business.

U.S. persons could implement risk assessment results to inform the development and refinement of their policies, procedures, training, and internal controls. Taking a robust approach, this risk assessment could identify potential areas for risk, including how and when the organization may engage in covered data transactions with covered persons or countries of concern. The risk assessment could examine the company's (i) current security measures; (ii) vendors, investors, and employees; (iii) offered products and services[18]; (iv) coverage under existing general or specific licenses or exemptions; and (v) the geographic locations of the organization, as well as its vendors, subsidiaries, parent organizations, intermediaries, and counterparties.

A company's Data Compliance Program should include internal controls, including written policies and procedures, that will identify, escalate, and report activity, as appropriate, and should minimize any risks identified in a company's risk assessment. These internal controls should also include a procedure for bringing newly acquired entities into compliance with the U.S. company's Data Compliance Program.

ii. Vendor Management and Validation

Second, under § 202.1001(b)(2), for restricted transactions that involve vendor agreements, the Data Compliance Program must include risk-based procedures for verifying the identity of vendors. Specifically, U.S. persons should screen vendors to verify whether current or prospective vendors are covered persons, as defined in § 202.211(a). For example, vendors may meet the definition of covered persons due to being located or headquartered in countries of concern or for being 50% or more owned, directly or indirectly, by such an entity. Covered persons designated by the Department pursuant to § 202.211(a)(5) will be added to the Covered Persons List and notice will be published in the Federal Register. Covered persons falling in the categories § 202.211(a)(1)-(4) do not require identification or designation by the Department and may not appear in the Covered Persons List. The Department may nonetheless identify some of these covered persons in the Covered Persons List to help improve compliance with the DSP.

Because persons or entities may be added to the Covered Persons List over time, an effective Data Compliance Program should adjust to these changes and include controls to screen vendors against the Covered Persons List periodically based on the company's risk appetite. Taking a robust approach, a U.S. entity's screening software could examine current or prospective vendors' geographical information to determine whether the vendor is located in, organized or chartered under the laws of, or has its principal place of business in a country of concern. Organizations that employ screening software should ensure such software (1) incorporates updates to the Covered Persons List, (2) accounts for all identifiers, including alternative spellings or AKAs of identified or designated covered persons; (3) accounts for organizational hierarchy; (4) considers vendors' geographical information (including

[18] A company is generally expected to "know their data", including the kind or volume of data processed or handled; how the company uses the data; whether the U.S. company engages in data transactions; and how such data is marketed, particularly with respect to current or recent former employees or contractors, or former senior officials, of the United States Government, including the military and Intelligence Community.

headquarters, subsidiary, and branch locations); and (5) screens against both current, newly added, and prospective vendors.

U.S. persons engaging in vendor agreements with foreign person entities ordinarily would not be expected, as part of their Data Compliance Program, to conduct due diligence on the employment practices of the foreign person entity to determine whether the foreign person entity's employees qualify as covered persons. It generally would not be a DSP violation for a U.S. person to engage in a vendor agreement to have bulk U.S. sensitive personal data or government-related data processed or stored by a foreign person that is not a covered person, even if that foreign person employs covered persons and grants them access to the data (absent any indication of evasion or knowing direction). However, under § 202.211(a)(3), when a vendor is a covered person entity, all the foreign-person employees of that vendor are covered persons as well.

Compliance with the DSP does not ensure compliance with other regulatory frameworks. For example, in addition to the Covered Persons List, U.S. persons should also screen vendors against other lists, as appropriate, including but not limited to:

- The Specially Designated Nationals and Blocked Persons list ("SDN List");
- The Sectoral Sanctions Identification List ("SSI List");
- Other sanctions-related lists administered by the Department of the Treasury's Office of Foreign Assets Control;
- The Entity List administered by the Department of Commerce's Bureau of Industry and Security;
- The Federal Communications Commission's Covered List;
- NDAA for Fiscal Year 2021 1260h list, as administered by the Department of Defense;
- Persons subject to a prohibition pursuant to E.O. 13873, Securing the Information and Communications Technology and Services Supply Chain; and
- Persons subject to a removal or exclusion order pursuant to the Federal Acquisition Supply Chain Security Act.

iii. Written Data Compliance Program Policy

A compliant Data Compliance Program must include a written policy that describes the data compliance program and that is annually certified by an officer, executive, or other employee responsible for compliance. For a robust approach, any written procedures should reflect the organization's day-to-day operations, should be easy to comply with, should make verification of compliance straightforward, and should be designed to prevent employees from engaging in misconduct. Ideally, companies should clearly communicate and confirm understanding of the Data Compliance Program's policies and procedures to all relevant staff, including, as appropriate, personnel within the company's compliance functions and relevant gatekeepers and business units (such as sales or vendor procurement teams and security personnel), and third parties performing relevant responsibilities on behalf of the organization.

As a best practice to develop a robust program, entities should consider including in their written Data Compliance Program policy internal controls that are developed based on risk assessment results, and that enable the organization to identify, escalate, and report to appropriate personnel any covered data transactions that may violate the DSP. Internal controls

may be most effective when they appoint and empower responsible compliance personnel and establish a formal escalation process to review high-risk transactions, including assessing whether there is a need to seek a specific license or Advisory Opinion from, or make a Voluntary Self-Disclosure to NSD. Annual review and certification of the Data Compliance Program's written policies and procedures must assess its adequacy and the effectiveness of its implementation.

iv. Written Security Requirements Policy

Each Data Compliance Program must include a written policy that describes the implementation of the security requirements, as defined in § 202.248. This written policy must be annually certified by an officer, executive, or other employee responsible for compliance. CISA's website provides additional information on the necessary Security Requirements.

2. Other Data Compliance Program Requirements

Under § 202.1001(b)(5), the Attorney General may require additional information in a Data Compliance Program. Any such requirements will be published in the Federal Register before they go into effect.

3. Training Personnel

Although not explicitly required by the DSP, U.S. persons conducting restricted transactions should consider providing periodic (ideally, at least annual) training on the Data Compliance Program and the CISA Security Requirements to all relevant employees and personnel. Training sessions and materials may be most effective if they:

- communicate the "why" of these requirements, including the underlying national security context;
- are developed according to the roles of the employees being trained;
- communicate the responsibilities for each employee and consequences of noncompliance; and
- hold employees accountable for compliance training through assessments.

Training could provide adequate information and instruction to employees and, as appropriate, stakeholders (for example, clients, vendors, business partners, and counterparties) to support the organization's compliance efforts. Such training could be further tailored for employees within the organization that are at a higher risk of being involved in covered data transactions. Training should be scoped appropriately to match the company's business risks and the geographic regions in which it operates or transacts, particularly when those regions include a country of concern or covered persons. The final rule provides several examples that could be used to train and test personnel understanding. Generally, all training materials should be maintained as an easily accessible internal resource for all employees. Following apparent violations or systemic deficiencies uncovered as the result of an audit or breach, or as identified by the organization during the routine course of business, U.S. persons should consider taking immediate action to provide training or take other corrective action with respect to relevant personnel and should amend periodic training as necessary and appropriate for other company personnel.

4. Audit Requirements

Audits assess the effectiveness of policies and procedures and can identify any inconsistencies between these controls and day-to-day operations. Carefully conducted audits can stop or prevent violations of the DSP by identifying breaches of procedures and deficiencies in an organization's Data Compliance Program. To detect compliance gaps, U.S. persons must audit their Data Compliance Program; their compliance with Security Requirements; and all related software, systems, and other technology. U.S. persons should use the results of those audits to enhance their Data Compliance Program and their security practices.

U.S. persons engaging in any restricted transactions must conduct comprehensive, independent, and objective audits, as delineated in § 202.1002. To minimize compliance burdens, U.S. persons may use audits completed for other purposes to comply with the DSP. The DSP 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 requirements set forth in the DSP.

This audit must be performed once for each calendar year in which the U.S. person engages in any restricted transaction and must cover the 12 months preceding the restricted transaction. Conducting periodic audits is useful to confirm whether compliance efforts are effective and can help U.S. persons adapt and recalibrate to changes to a U.S. person's risk environment and appetite. Ideally, companies' internal controls should identify which senior management personnel are responsible for ensuring timely audits are conducted.

There are several key requirements for the person(s) conducting the audit. The auditor must be qualified and competent to examine, verify, and attest to the U.S. person's compliance with and the effectiveness of the Security Requirements, as defined in § 202.248, and all other applicable requirements under subpart J. The auditor must also be independent and should be objective, fact-based, nonpartisan, and nonideological with regards to both the U.S. person and to the transactions that are subject to the audit. The auditor should not be involved in the transaction or associated with, owned, or controlled by any person who is party to or otherwise involved in the transaction they are auditing. The auditor's objectivity in discharging their professional responsibilities is the basis for the credibility of auditing in the government and private sectors. Optimally, the auditor should have sufficient skills, resources, and expertise and should maintain ethical principles to complete the audit. Finally, the auditor cannot be a covered person, as defined in § 202.211, or a country of concern, as defined in § 202.209.

The DSP does not require compliance with specific auditing standards. The Government Accountability Office (GAO) provides guidance regarding qualifications for performing program and financial statement audits in the "Generally Accepted Government Auditing Standards" (Yellow Book), but an auditor could alternatively, for example, adhere to standards established by (1) the Public Company Accounting Oversight Board (PCAOB) or (2) the International Auditing and Assurance Standards Board (IAASB). Auditors should use a reliable methodology that employs testing or audit procedures, that are appropriate to the level and sophistication of the subject U.S. person entity, and that reflect a comprehensive and objective assessment of the entity's practices.

The audit must examine the U.S. person's data transactions; compliance with CISA Security Requirements; Data Compliance Program; and relevant records, as delineated by the

recordkeeping requirements in § 202.1101. Within 60 days of the audit's completion, the auditor must prepare and submit a report on findings to a senior officer of the company, preferably a compliance officer responsible for general cybersecurity or compliance with the DSP. The required contents of this audit report are listed in § 202.1002(f). In accordance with recordkeeping requirements in § 202.1101, U.S. persons must retain each audit report for a period of at least ten years. Upon receipt of a qualified, adverse, or "disclaimer of opinion" audit finding, the U.S. person should ideally take immediate and effective action to identify and implement compensating controls that address the root causes of any issues. U.S. persons should also ideally take steps to conduct and document efforts to remediate any deficiencies uncovered by the audit. Consistent with § 202.302(b), U.S. persons must disclose violations of the Data Security Program to NSD. NSD may request that U.S. persons furnish audit reports on demand, as provided in § 202.1102.

C. Recordkeeping and Reporting Requirements

1. Recordkeeping Requirements

The DSP recordkeeping requirements are contained in § 202.1101. Except as otherwise provided, U.S. persons engaging in any transaction subject to the DSP should keep a full and accurate record of each such transaction engaged in, and such record should be available for examination for at least ten years after the date of such transaction. Section 202.1101(b) lists the records that U.S. persons are obligated to create and maintain in an auditable manner.

As discussed below in Part IV(D), a senior official at the U.S. entity must sign an annual certification of the completeness and accuracy of the company's recordkeeping, as supported by an audit. Proper recordkeeping can provide clear historical data that can facilitate trend analysis, strategic planning, and identification of Data Compliance Program programmatic weaknesses.

U.S. persons should familiarize themselves with when the recordkeeping requirements of § 202.1101 apply. First, the recordkeeping requirements apply to any non-exempt covered data transaction. Second, the recordkeeping requirements apply to covered data transactions authorized by a general or specific license. In some instances, general and specific licenses may impose additional or different recordkeeping requirements. Third, the recordkeeping requirements set forth in § 202.1101(a) apply to covered data transactions conducted in accordance with the exemption in § 202.510 for certain drug, biological product, and medical device authorizations.

The recordkeeping requirements do not apply to any data transactions conducted in accordance with the following exemptions: official business of the United States Government (§ 202.504), financial services (§ 202.505), corporate-group transaction (§ 202.506), transactions required or authorized by Federal law or international agreements, or necessary to comply with Federal law (§ 202.507), investment agreements subject to a CFIUS action (§ 202.508), telecommunications services (§ 202.509), and clinical investigations and post-marketing surveillance data (§ 202.511).

2. Reporting Requirements

Sections 1102, 1103, and 1104 also impose certain reporting requirements. Section 202.1102 requires every person to furnish under oath, in the form of reports or otherwise, from

time to time and at any time as may be required by NSD, complete information relative to any act or covered data transaction, regardless of whether such act or covered data transaction is affected pursuant to license or otherwise, subject to the provisions of subpart K. Section 202.1103 describes annual reporting obligations for persons engaged in certain restricted transactions, as further discussed in Part IV(E) below. Section 202.1104 concerns reporting requirements for rejected prohibited transactions involving data brokerage, which do not apply to restricted transactions.

D. Involvement of Senior Management and Compliance Personnel

Senior managers should endeavor to promote a culture of accountability across their organization and to require personnel to respond effectively to violations of the DSP. A robust Data Compliance Program should have senior management support and buy-in. U.S. companies should appoint an individual responsible for building and maintaining the compliance program. Compliance managers should have organizational senior-level authority, sufficient technical expertise, and should be provided appropriate personnel, technical, and other resources to ensure proper implementation of the Data Compliance Program. Compliance managers should build a team that is empowered to integrate the Data Compliance Program's controls into the company's daily operations and ensure that employees have adequate training and job-specific knowledge regarding the Data Security Program and the company's relevant policies. These personnel should regularly test these controls and remediate any weaknesses or gaps as described above. The composition and roles of senior management and compliance personnel in implementing the DSP will vary based on the facts and circumstances of each U.S. person's exposure to DSP-related risks.

As mentioned above, an officer, executive, or other employee responsible for compliance should sign an annual certification of (1) the company's Data Compliance Program implementation and due diligence efforts; (2) the company's implementation of any applicable security requirements as defined in § 202.248; and (3) the completeness and accuracy of recordkeeping documenting the company's due diligence, as supported by an audit. The responsible employee should not be a covered person. This certification process is an opportunity for senior management to reassess the Data Compliance Program and report conclusions about the effectiveness of the company's internal controls. Ideally, through this written document, the senior personnel should also certify:

- Whether the company has in place processes to establish, maintain, review, test, and modify written compliance policies and written supervisory procedures that are reasonably designed to achieve compliance with the Data Security Program;
- That the above attestation is evidenced in a report that has been reviewed by the chief executive officer and that a final report has been submitted to the company's board of directors and audit committee;
- Whether there were significant changes in internal controls or in other factors that could significantly impact internal controls subsequent to the date of the report's evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses;
- That, based on the officer's knowledge, the report does not contain any untrue statement of material fact, and does not omit any material facts;

- Whether compliance personnel have conducted one or more meetings with the chief executive officer(s) in the preceding 12 months to discuss compliance with the DSP; or
- That the chief executive officer has consulted with the chief compliance officer(s), other officers as applicable, and other employees, outside consultants, lawyers, auditors, and accountants, to the extent deemed appropriate, in order to verify the statements made in this certification.

Under subpart K of the DSP, annual certifications should be retained and furnished to NSD upon request. The failure to annually certify and provide such certifications in a U.S. person's annual report when the person is engaged in restricted transactions may constitute a violation of the Data Security Program and could be considered a factor in NSD's analysis of possible enforcement action.

E. Annual Reporting Requirement

Certain U.S. persons (or their attorney, agent, or other representative[19]) engaged in the data transactions described in § 202.1103(a) may be required to file an annual report describing such transactions engaged in during the previous calendar year. Such reports must be filed by March 1 of the year following the year of the report. This requirement applies to any U.S. person that is engaged in a restricted transaction involving cloud-computing services, and that has 25% or more of the U.S. person's equity interests owned (directly or indirectly, through any contract, arrangement, understanding, relationship, or otherwise) by a country of concern or covered person.

The required contents of this report are listed in § 202.1103(d). NSD may request additional or follow up information to supplement submitted annual reports. Submissions must be made to NSD electronically, in accordance with § 202.1201, by emailing nsd.firs.datasecurity@usdoj.gov or using another official electronic reporting option, in accordance with any instructions on the National Security Division's website. NSD will not accept paper copies of annual reports.

V. Exempt Transactions

Subpart E of the DSP provides a list of several exempt transactions to which subparts C, D, J and K (other than §§ 202.1102 and 202.1104) do not apply to the extent the listed criteria are met. U.S. persons engaging in covered data transactions pursuant to subpart E should take note that the U.S. persons may still be obligated to comply with certain recordkeeping and reporting requirements for any covered data transaction conducted pursuant to the exemptions for official business of the United States Government (§ 202.504), financial services (§ 202.505); corporate group transactions (§ 202.506); transactions required or authorized by Federal law or international agreements, or necessary to comply with Federal law, (§ 202.507); investment agreements subject to a CFIUS action, § 202.508; telecommunications services (§ 202.509); and certain drug, biological product, and medical device authorizations, and other clinical investigations and post-marketing surveillance data (§§ 202.510 and 202.511). U.S. persons that

[19] Primary responsibility for reporting rests with the actual U.S. person engaging in the data transaction. No U.S. person is excused from filing a report by reason of the fact that another U.S. person has submitted a report with regard to the same data transaction, except where the U.S. person has actual knowledge that the other U.S. person filed the report.

are unsure whether an exemption may apply to their prospective activity may submit a request for an advisory opinion.

VI. Licensing

A license is an authorization from NSD to engage in a covered data transaction that otherwise would violate the Data Security Program. There are two types of licenses: general licenses and specific licenses. A general license authorizes a particular type of transaction for a class of persons without the need to apply for a specific license. A specific license is a written document issued by NSD to a particular person or entity, authorizing a particular transaction or transactions in response to a license application.

As noted in Part II.A above, 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. 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).

A. General Licenses

NSD has discretion to issue general licenses to authorize certain covered data transactions that would otherwise violate the Data Security Program. 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. Persons engaging in transactions pursuant to general licenses must ensure that all terms and conditions are strictly observed, including but not limited to reporting requirements. NSD will publish any general licenses on its website and to the Federal Register. Some general licenses may be time limited and provide an expiration date by which U.S. persons are expected to cease covered activity.

B. Specific Licenses

Entities may apply for a specific license authorizing particular covered data transactions with a covered person or country of concern. 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). NSD will consider the issuance of specific licenses on a case-by-case basis when a general license provision is not applicable.

NSD's primary mission with respect to the administration and enforcement of the Order and the DSP is protecting U.S. national security from countries of concern that may seek to

collect and exploit Americans' most sensitive personal 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 U.S. government-related data and Americans' bulk sensitive personal data, NSD applies a "presumption of denial" standard for all specific license applications. 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.

A specific license is not transferable, is limited to the facts and circumstances specific to the application, and is subject to the provisions of 28 CFR part 202 and the Order. A license may be revoked or modified at any time at the discretion of NSD. Persons engaging in transactions pursuant to a specific license must ensure that all terms and conditions are strictly observed, including but not limited to reporting requirements. Making false or misleading statements on or in connection with a license application may constitute serious criminal or civil violations of Federal law and may result in substantial fines or other sanctions.[20] If a specific license was issued as a result of willful misrepresentation on the part of the applicant or his agent, it may, at the discretion of NSD, be declared void from the date of its issuance, or from any other date.

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

VII. Advisory Opinions

Section 202.901 creates a mechanism for NSD to provide further information to the public on the applicability of the DSP in the form of written advisory opinions. Potentially regulated parties may seek advisory opinions regarding the application of the DSP to specific transactions. These advisory opinions represent the present enforcement intentions of NSD with respect to the specific transactions identified, but do not create substantive or procedural rights, privileges, or benefits enforceable in any administrative, civil, or criminal matter.

As noted in § 202.901(b), requests must be submitted by a U.S. person party to the transaction or that party's agent. Requests do not apply to a party that does not join the request. Advisory opinion seekers must submit requests that include all material information that bears on the prospective conduct and circumstances for which the advisory opinion is requested. Section 202.901(c) lists the required content for a complete advisory opinion request. Generally, NSD must receive all relevant background information, copies of all operative documents, and detailed statements of all collateral or oral understandings between parties to the transaction. Requests must be accompanied by a certification that the request and all accompanying materials are truthful and accurate consistent with 18 USC § 1001.

NSD may retain any advisory opinion request, document, or information submitted to it under this procedure or otherwise; disclose any advisory opinion and advisory opinion request,

[20] Attention is directed to 18 U.S.C. § 1001 and section 701 et seq. of the relevant part of 28 CFR for provisions relating to penalties.

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; or use any such request, document, or information for any governmental purpose.

As noted in Part II.A above, 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. 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).