

January 17, 2025

# DOJ Issues Final Rule Restricting the Transfer of Certain Sensitive U.S.-Person Data

On December 27, 2024, the United States Department of Justice's ("DOJ") National Security Division promulgated a final rule implementing President Biden's February 2024 executive order on bulk sensitive data, titled "Preventing Access to Americans' Bulk Sensitive Data and United States Government-Related Data by Countries of Concern" (the "Order").<sup>1</sup> The Rule restricts or prohibits the provision of U.S. persons' data to covered persons or countries of concern (including China) and imposes due diligence and security obligations on companies that engage in certain restricted transactions. A senior Department of Justice official stated: "[t]his powerful new national-security program is designed to ensure that Americans' personal data is no longer permitted to be sold to hostile foreign powers, whether through outright purchase or other means of commercial access."<sup>2</sup>

The Rule will become effective on April 8, 2025, and entities must comply with the Rule's due diligence, audit and reporting requirements by October 5, 2025.<sup>3</sup> The Rule does not apply to transactions completed before its effective date, but it does apply to ongoing activity, even if that activity is required by prior contracts.<sup>4</sup> DOJ will continue to engage with stakeholders in the run-up to April 8, and may offer licenses for companies to take additional time to wind down activities.<sup>5</sup>

The Rule is the culmination of DOJ's swift rule-making process. On February 28, 2024, President Biden issued the Order to address the national security threat identified by the Administration posed by foreign adversaries' efforts to access and exploit the sensitive data of U.S. persons.<sup>6</sup> The Order instructed the Attorney General to issue regulations to advance the President's central objective of "restrict[ing] access by countries of concern to Americans' bulk sensitive personal data and United States Government-related data when such access would pose an unacceptable risk to the national security of the United States."<sup>7</sup> On

---

<sup>1</sup> Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, to be codified at 28 C.F.R. Part 202, available [here](#).

<sup>2</sup> See U.S. Dep't of Just., Press Release: Justice Department Issues Final Rule Addressing Threat Posed by Foreign Adversaries' Access to Americans' Sensitive Personal Data (Dec. 27, 2024), available [here](#).

<sup>3</sup> See Rule at 1 (90-day effective date), 32 (270-day compliance requirement).

<sup>4</sup> *Id.* at 38-39.

<sup>5</sup> *Id.* at 37.

<sup>6</sup> The White House, *Executive Order 14117 on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern* (Feb. 28, 2024) ("Executive Order 14117"), available [here](#); see also Paul, Weiss, *Invoking National Security Risks, President Biden Issues Executive Order Restricting the Transfer of Certain Sensitive U.S. Personal Data to Countries of Concern* (Feb. 29, 2024), available [here](#).

<sup>7</sup> *Executive Order 14117*.

March 5, 2024, DOJ published an Advanced Notice of Proposed Rulemaking, and published a Notice of Proposed Rulemaking on October 21, 2024.<sup>8</sup>

## Key Takeaways

**Broad Scope.** The Rule affects the types of partnerships and arrangements that U.S. companies are able to engage in with Chinese companies, and it is likely to implicate a large number of U.S. companies that conduct business internationally. In addition to creating an outright prohibition on certain data-related transactions, a broad range of other transactions are “restricted.” Restrictions on transactions involving vendor, employment, and non-passive investment agreements, together with their attendant reporting obligations, will require companies to carefully monitor their transactions to ensure compliance with the Cybersecurity and Infrastructure Security Agency (“CISA”) security requirements. DOJ expects U.S. persons engaged in transactions within the rule’s scope to ensure that foreign counterparties are complying with the rule, and a U.S. person’s failure to conduct due diligence regarding its counterparties can constitute a violation of the rule.<sup>9</sup>

**Prepare in Advance.** A senior Department of Justice official has provided four points of advice to companies: (1) know your data, (2) know where that data is going, (3) know who has access to the data and (4) know your data sales.<sup>10</sup> Given the breadth of the Rule’s application, implementing this advice may be critical for complying with the Rule. Companies will also need to consider including specific contractual restrictions in agreements with foreign counterparties to ensure compliance with these new rules, and may need to consider adjusting diligence processes, contractual frameworks and data oversight programs in order to fully comply with the rule, once finalized. Specifically, entities engaging in restricted transactions will need to adopt the specific compliance procedures articulated in the Rule. DOJ will consider the strength of a given compliance program when determining whether to pursue an enforcement action or the magnitude of any enforcement action.

Additionally, businesses should consider the Rule’s second-order effects. For instance, Chinese companies looking to establish a footprint in U.S. markets may be limited to industries where data covered by the Rule would be less prevalent. This limitation could impact market dynamics in key industries including healthcare, defense, telecommunications and other critical sectors.<sup>11</sup>

**Notable Changes from the NPRM.** Three of the changes that DOJ implemented in response to feedback from the NPRM are particularly notable. First, DOJ clarified that “a U.S. person accessing data from a covered person ordinarily does not present the national security concerns that the rule seeks to address, and the Department does not intend the rule to cover that generic circumstance.” Second, the DOJ “amended the definition of ‘data brokerage’ to explicitly exclude an employment, investment, or vendor agreement,” which ensures that “the categories of prohibited transactions and restricted transactions remain mutually exclusive.” Third, the final rule provides that the provision of AI-generated information based on bulk covered personal identifiers to a covered person or country of concern could itself constitute a prohibited data brokerage transaction if the covered person or country of concern knows the algorithm and can use it to reveal the underlying personal identifiers.<sup>12</sup>

## The Rule

The Rule prohibits or restricts U.S. persons from engaging in “covered transactions” with “covered persons” that involve U.S. persons’ “bulk sensitive personal data” or government-related data. Covered transactions are data brokerage, as well as those

---

<sup>8</sup> NPRM on Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, C.F.R. Part 202, Docket No. NSD 104, available [here](#); see also Paul, Weiss, *DOJ Issues Notice of Proposed Rulemaking Restricting the Transfer of Certain Sensitive U.S.-Person Data* (Nov. 18, 2024), available [here](#).

<sup>9</sup> Rule at 338, § 202.401(a).

<sup>10</sup> Dep’t of Justice, *Assistant Attorney General Matthew G. Olsen Delivers Keynote Speech at the American Bar Association’s 39th National Institute on White Collar Crime* (Mar. 8, 2024), available [here](#).

<sup>11</sup> See generally, John Carlin et al., *Bulk Sensitive Data Transfer Rule Would Tighten Security Controls*, BLOOMBERG (Mar. 19, 2024), available [here](#).

<sup>12</sup> Rule at 41. See *id.* at 291, § 202.210, *example 3* (U.S. person receiving data from covered persons); *id.* at 44. See *id.* at 300, § 202.214(b)(7) & (8) (data brokerage definitions); Rule at 334, § 202.304(b)(5) (AI provisions).

under vendor, employment and investment agreements. Data brokerage transactions are prohibited, while the latter three are restricted. While the Rule does not impose generally applicable due diligence procedures, it requires entities engaging in restricted transactions to comply with security requirements as promulgated by CISA.<sup>13</sup>

### 1. “Countries of Concern” and “Covered Persons”

The Rule identifies six “countries of concern”: China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia and Venezuela. The Rule permits the Attorney General, with the concurrence of the Secretary of the Treasury and Secretary of Commerce, to add countries to this list if they meet the criteria.<sup>14</sup>

The Rule defines “covered person” in four categories:

- (a) Foreign persons that are entities that are 50 percent or more owned by one or more countries of concern and/or Covered Persons, organized under the laws of a country of concern, or have their principal place of business in a country of concern;
- (b) Foreign persons that are entities and are 50 percent or more owned by a covered person;
- (c) Foreign persons who are individuals and who are employees or contractors of countries of concern or entities that are covered persons; and
- (d) Foreign persons who are individuals and who are primarily resident in countries of concern.<sup>15</sup>

Under the Rule’s terms, therefore, entities may qualify as “covered persons” without being physically located in the territory of a country of concern.

“Covered persons,” however, do not include “U.S. persons,” who are defined as any U.S. citizen, national or lawful permanent resident, as well as any entity organized in the United States, or any person located in the United States.<sup>16</sup> Thus, U.S. subsidiaries of covered persons would not themselves be covered persons.

### 2. Prohibited and Restricted Data Transactions

The Rule regulates certain transactions that involve U.S. persons’ “sensitive personal data” that exceeds a “bulk” threshold. It also prohibits or restricts certain transactions that involve government-related data.

**Sensitive Personal Data.** “Sensitive personal data” is data that falls into these six categories:<sup>17</sup>

- (a) Two or more enumerated identifiers (defined as device-based identifiers like IMEIs, MAC addresses or SIM card numbers, or social security numbers, driver’s licenses or other government identification numbers) together, or a single enumerated identifier in “combination with other data that is disclosed by a transacting party pursuant to the

---

<sup>13</sup> See Security Requirements for Restricted Transactions, CISA (Jan. 2025), available [here](#).

<sup>14</sup> Rule at 362, § 202.601(a) (list of countries of concern); *id.* at 289-90, § 202.209 (power to amend).

<sup>15</sup> *Id.* at 291, § 202.211(a). Additionally, the Attorney General can publicly designate a person or entity as a “covered person” under certain circumstances. *Id.* at 291-92, § 202.211(a)(5).

<sup>16</sup> *Id.* at 304, § 202.221 (“The term foreign person means any person that is not a U.S. person.”); *id.* at 324-25, § 202.256(a).

<sup>17</sup> *Id.* at 322, § 202.249(a) (listing categories); *see also id.* at 294, § 202.212(a) (defining “covered personal identifiers”); *id.* at 320, § 202.242 (defining “precise geolocation data”); *id.* at 287, § 202.204 (defining “biometric identifiers”); *id.* at 306-07, § 202.224 (defining “human ‘omic data”); *id.* at 319-20, § 202.241 (defining “personal health data”); *id.* at 319, § 202.240 (defining “personal financial data”).

transaction such that the listed identifier is linked or linkable to other listed identifiers or to other sensitive personal data;”

- (b) Precise geolocation data;
- (c) Biometric identifiers (facial images, voice prints and patterns, and retina scans);
- (d) Human ‘omic data (i.e. genomic, epigenomic, proteomic, or transcriptomic data);
- (e) Personal health data (height, weight, vital signs, symptoms, test results, diagnosis and psychological diagnostics); and
- (f) Personal financial data (information related to an individual’s credit, debit cards, bank accounts and financial liabilities, including payment history).

“Sensitive personal data” does not include public and nonpublic data that does not relate to an individual (e.g., trade secrets and proprietary information), data that is already legally public from government records or that is distributed widely via media, and personal communications.<sup>18</sup>

**Bulk threshold.** The Rule prohibits transactions involving “sensitive personal data” that surpass a “bulk” threshold. Here, “bulk” means any amount of covered data, regardless of whether such data is anonymized, pseudonymized, de-identified or encrypted, that, in the aggregate, exceeds various specific thresholds over the 12 months before a covered data transaction:<sup>19</sup>

Type	Human ‘Omic Data	Human Genomic Data	Biometric Identifiers	Precise Geolocation Data	Personal Health Data	Personal Financial Data	Certain Covered Personal Identifiers <sup>20</sup>
Threshold	Over 1,000 U.S. persons	Over 100 persons	Over 1,000 U.S. persons	Over 1,000 U.S.. devices	Over 10,000 U.S. persons		Over 100,000 U.S. persons

**U.S. Government-Related Data.** The Rule also restricts or prohibits certain transactions with U.S. government-related data. Government-related data means: (1) any precise geolocation data for a location within a list of locations which the Attorney General has determined poses a heightened risk (such as a workplace for federal government employees who work in national security, a military installation, or facilities that otherwise support the government’s security-related functions) or (2) sensitive personal data that a transacting party markets as linked or linkable to current or former government employees. The bulk thresholds do not apply to transactions involving government-related data. The proposed rule therefore applies to covered transactions of government-related data no matter the volume of data.<sup>21</sup>

<sup>18</sup> *Id.* at 322, § 202.249(b).

<sup>19</sup> *Id.* at 287-88, § 202.205

<sup>20</sup> *Id.* at 294, §§ 202.212 (a) & (b). A covered personal identifier is any identifier used “[i]n combination with any other listed identifier” or “[i]n 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,” other than “[d]emographic or contact data that is linked only to other demographic or contact data” and “[a] network-based identifier, account-authentication data, or call-detail data as necessary for the provision of telecommunications, networking, or similar service.”

<sup>21</sup> *See id.* at 304-305, § 202.222(a)(1) (articulating rule); *id.* at 390-421, § 202.1401 (providing the government-related location data list); *id.* at 305, § 202.222(a)(2).

### 3. Covered Data Transactions

The Rule defines a “covered data transaction” as any transaction that involves government-related data or U.S. persons’ bulk sensitive data that involves (1) a data brokerage, (2) a vendor agreement, (3) an employment agreement or (4) an investment agreement.<sup>22</sup> Under the Rule, “covered data transactions” are either prohibited or restricted, except for certain exemptions.

**Prohibited Transactions.** The Rule prohibits U.S. persons from engaging in data brokerage of U.S. persons’ bulk sensitive personal data, or government-related data, with a covered person.<sup>23</sup> Furthermore, any transaction with any foreign person of bulk sensitive personal data or government-related data must include a provision that the foreign person will not provide access to a covered person.<sup>24</sup> The Rule also prohibits transactions that have “the purpose of evading or avoiding . . . any of the prohibitions set forth in this part” and “[k]nowingly directing prohibited or restricted transactions.”<sup>25</sup>

**Restricted Transactions.** Outside of prohibited transactions, the Rule restricts three categories of covered data transactions with countries of concern or covered persons: vendor agreements, employment agreements and non-passive investment agreements. As previewed in the NPRM, the Rule also sets a 10% *de minimis* threshold for investments to qualify as covered transactions. As a result, data transactions under investment agreements that give the covered person less than 10% in total voting and equity interest, do not qualify as restricted. Otherwise, entities may engage in restricted transactions only if they comply with applicable CISA security requirements.<sup>26</sup>

**Exempt Transactions.** The Rule exempts transactions involving eleven classes of data entirely:<sup>27</sup>

- Personal communications;
- Information or informational materials related to exports and imports;
- Transactions incident to travel to or from a country;

---

<sup>22</sup> *Id.* at 290, § 202.210(a).

<sup>23</sup> *Id.* at 328, § 202.301(a). “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.” *Id.* at 298, § 202.214(a).

<sup>24</sup> DOJ notes that it anticipates publishing guidance in the near future that provides model contractual language that entities can use to satisfy this requirement. U.S. Dep’t of Just., Press Release, at 5, *supra*.

<sup>25</sup> *Id.* at 329-30, § 202.302(a). DOJ notes that it anticipates publishing guidance in the near future that provides model contractual language that entities can use to satisfy this requirement. U.S. Dep’t of Just., Press Release, at 5, *supra*. Furthermore, as previewed in the NPRM, the Rule prohibits *any* covered transaction (i.e. any of the four transaction types above) involving human ‘omic data or human biospecimens from which human ‘omic data can be derived, over the bulk threshold with a country of concern or covered person. *Id.* at 331-32, § 202.303 (transactions with foreign persons). *Id.* at 332, § 202.304(a); *id.* at 335, § 202.305(a).

<sup>26</sup> *Id.* at 338, § 202.401(a) (listing categories of restricted transactions). **Vendor Agreements** are defined as “[a]ny agreement or arrangement, other than an employment agreement, in which any person provides goods or services to another person, including cloud-computing services, in exchange for payment or other consideration.” *Id.* at 326, § 202.258(a). **Employment Agreements** are defined as “any agreement or arrangement in which an individual, other than as an independent contractor, performs work or performs job functions directly for a person in exchange for payment or other consideration, including employment on a board or committee, executive-level arrangements or services, and employment services at an operational level.” *Id.* at 302, § 202.217(a). **A non-passive Investment Agreement** is an investment agreement that provides a foreign technology company with enough of an ownership interest that it can become involved in substantive business and strategy decisions. Where the investment agreement would involve the ability to access bulk U.S. sensitive personal data, it is a restricted transaction. *Id.* at 310-12, § 202.228(b), *Example 3*. Agreements that give the covered person less than 10% in total voting and equity interest are considered passive under the Rule. *Id.* at 310, § 202.228(b)(2). *Id.* at 321-22, § 202.248; *see also* Security Requirements for Restricted Transactions, CISA, *supra*.

<sup>27</sup> *Id.* at 339-62, §§ 202t.501-202.511.

- Official U.S. Government activities;
- Financial services, including investment management services, if the transactions are ancillary to those services;<sup>28</sup>
- Corporate group transactions between U.S. entities and a foreign subsidiary or affiliate, so long as the transactions are part of ordinary business operations, (e.g., payroll, customer support, human resources, etc.);
- Transactions required or authorized by international agreements or federal law;
- Investment agreements, if CFIUS designates them as exempt or subjects the transactions to mitigation;
- Transactions necessary to provide telecommunications services, (e.g., data roaming and mobile voice calls);
- Drug, biological product and medical device authorizations if transactions involve “regulatory approval data,” which is data that must be produced to a regulator before a business can research or market a drug, device or other biological product; and
- FDA clinical investigations.

#### 4. Notable Changes from the NPRM

As noted above, the Rule maintains the NPRM’s general framework and key definitions. However, it contains three notable changes from the NPRM, as follows:

- (a) **Clarification of the scope of Covered Transactions.** The Rule clarifies that the provision of U.S. persons’ bulk sensitive personal data already in the possession of a covered person or a country of concern to a U.S. person is not a covered transaction. Previously, the NPRM had defined “covered data transactions” as involving “any access to any government-related data or bulk U.S. sensitive personal data,” regardless of by whom, and therefore it had been unclear whether the proposed rule would regulate access of relevant data provided by a covered person to a U.S. person. Now, the Rule defines “covered data transactions” as those relevant transactions involving “access by a country of concern or covered person to any government-related data or bulk U.S. sensitive personal data,” and as explained in the Rule, transactions where covered persons already possess the data do not implicate granting them access.<sup>29</sup> Thus, transactions involving access by a U.S. Person to relevant data are not “covered data transactions.”
- (b) **Clarification of the interaction between prohibited and restricted transactions.** The Rule further provides that restricted transactions are mutually exclusive with transactions prohibited as data brokerage. As a result, transactions controlled by vendor, employment or passive investment agreements cannot qualify as data brokerage. Nonetheless, the Rule leaves open the possibility that there may be certain types of ostensibly restricted transactions that are no longer feasible in practice by virtue of the CISA security requirements and thus effectively prohibited.<sup>30</sup>
- (c) **AI risk.** In the Rule’s provision that regulates knowing evasion of its requirements, the Rule adds a new example related to the risk posed by artificial intelligence. The example states that providing an “artificial intelligence algorithm” which has been trained on bulk covered personal identifiers may constitute a transaction prohibited as data brokerage if the

---

<sup>28</sup> Within the previously-proposed financial services exemption, the Rule now adds that transactions including data incident to the “trading and underwriting of securities, commodities, and derivatives” qualify as exempt transactions not subject to the Rule’s regulations. *Id.* at 342, § 202.505.

<sup>29</sup> NPRM on Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, at 329, § 202.210, *supra*; Rule at 290, § 202.210 (emphasis added); *see also id.* at 41 (explaining this clarification).

<sup>30</sup> *Id.* at 298, § 202.214; *id.* at 44.

covered person or country of concern can use it to access underlying personal identifiers in the training data.<sup>31</sup> As previously stated in the NPRM, liability under this section is limited to those actions purposefully taken to evade the regulation.

## 5. Guidance and Advisory Opinions

The Rule permits DOJ to issue general public guidance through agency responses to frequently asked questions, and also authorizes DOJ to issue advisory opinions addressing how the regulations would apply to specific proposed transactions.<sup>32</sup> Regulated parties can request advisory opinions on specific transactions but not on hypothetical scenarios.

## 6. Penalties and Reporting/Recordkeeping Requirements

**Compliance Obligations.** The Rule imposes three compliance obligations on U.S. persons who engage in restricted transactions. First, each U.S. person engaging in restricted transactions must develop and implement a data compliance program. This program must (1) verify and log data relevant to compliance with the Rule, (2) implement risk-based procedures for verifying the identity of vendors, (3) include a written policy that describes the data compliance program, (4) include a written policy describing implementation of the security requirements, and (5) incorporate any further requirements. Second, each U.S. person engaging in restricted transactions must undergo an annual audit. While the audit must be independent, the auditor may be internal, and DOJ will provide additional guidance on the requirements for a sufficiently independent audit. Third, each U.S. person engaging in restricted transactions must maintain a full and accurate record of each transaction and of its compliance program. DOJ will publish subsequent guidance about voluntary self-disclosures.<sup>33</sup>

**Reporting Requirements.** The Rule requires U.S. persons to furnish complete information to the Justice Department about any restricted act or transaction, regardless of whether it was effected pursuant to a license. Separately, any U.S. person engaged in a restricted transaction related to cloud computing, and that is 25% or more owned by a country of concern or covered person, must submit an annual report. Any U.S. person who has received and rejected an offer from another person to engage in a prohibited transaction must file a report to the Justice Department within 14 days.<sup>34</sup>

**Enforcement.** The civil and criminal penalties for violating the Rule are specified in Section 206 of IEEPA, 50 U.S.C. § 1705. The maximum civil penalty is \$368,136, while the maximum criminal penalties are a fine of \$1,000,000 and 20 years of imprisonment. The Justice Department is required to provide a pre-penalty notice and opportunity to respond before seeking civil penalties, and an alleged violator has the right to seek judicial review of the department's determinations.<sup>35</sup>

\* \* \*

---

<sup>31</sup> *Id.* at 334, § 202.304, *Example 5*.

<sup>32</sup> *Id.* at 370-74, § 202.901.

<sup>33</sup> *Id.* at 374-75, § 202.1001; *id.* at 375-77, § 202.1002; *id.* at 245; *id.* at 377-78, § 202.1101 (compliance requirements); *id.* at 257 (subsequent guidance).

<sup>34</sup> *Id.* at 378-79, § 202.1102 (publication requirements); *id.* at 380-81, § 202.1103 (cloud computing); *id.* at 382-83, § 202.1104 (reporting suspect transactions).

<sup>35</sup> *Id.* at 384-85, § 202.1301 (maximum fines and penalties); *id.* at 386-390, §§ 202.1302–1306 & 1401 (right to judicial review).

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

**L. Rush Atkinson**  
+1-202-223-7473  
[ratkinson@paulweiss.com](mailto:ratkinson@paulweiss.com)

**John P. Carlin**  
+1-202-223-7372  
[jcarlin@paulweiss.com](mailto:jcarlin@paulweiss.com)

**Roberto J. Gonzalez**  
+1-202-223-7316  
[rgonzalez@paulweiss.com](mailto:rgonzalez@paulweiss.com)

**Anna R. Gressel**  
+1-212-373-3388  
[agressel@paulweiss.com](mailto:agressel@paulweiss.com)

**David K. Kessler**  
+1-212-373-3614  
[dkessler@paulweiss.com](mailto:dkessler@paulweiss.com)

**Mark F. Mendelsohn**  
+1-212-373-3337  
[mmendelsohn@paulweiss.com](mailto:mmendelsohn@paulweiss.com)

**Nicole Succar**  
+1-212-373-3624  
[nsuccar@paulweiss.com](mailto:nsuccar@paulweiss.com)

**Peter Carey**  
+1-202-223-7485  
[pcarey@paulweiss.com](mailto:pcarey@paulweiss.com)

**Samuel Kleiner**  
+1-212-373-3797  
[skleiner@paulweiss.com](mailto:skleiner@paulweiss.com)

**Nathan Mitchell**  
+1-202-223-7422  
[nmitchell@paulweiss.com](mailto:nmitchell@paulweiss.com)

**Audrey M. Paquet**  
+1-212-373-2397  
[apaquet@paulweiss.com](mailto:apaquet@paulweiss.com)

*Associates Theodore Furchtgott and Samuel Rebo contributed to this Client Alert.*

## Our National Security Group

Paul, Weiss’s National Security Practice is the market leader on the most challenging national security, sanctions and export controls issues, as well as FARA and CFIUS matters. Our team includes several renowned national security lawyers and others who served as the top national security officials at the highest levels of government, and offers practical, commercial guidance and insights on navigating the national security landscape. Leveraging one of the industry’s deepest benches of regulatory defense and crisis management specialists, we are also experienced in regulatory and compliance counseling, transactional due diligence, and sensitive internal and government investigations and enforcement actions.

## Our National Security Partners

<a href="#">L. Rush Atkinson</a>	<a href="#">Jessica S. Carey</a>	<a href="#">John P. Carlin</a>	<a href="#">Roberto J. Gonzalez</a>
<a href="#">Melinda Haag</a>	<a href="#">Jeh Charles Johnson</a>	<a href="#">Brad S. Karp</a>	<a href="#">David K. Kessler</a>
<a href="#">Loretta E. Lynch</a>	<a href="#">Mark F. Mendelsohn</a>	<a href="#">Jeannie S. Rhee</a>	<a href="#">Nicole Succar</a>