FACT SHEET: Justice Department Issues Final Rule to Address Urgent National Security Risks Posed by Access to U.S. Sensitive Personal and Government-Related Data from Countries of Concern and Covered Persons

Today, the Justice Department issued and publicly posted a final rule to address the national-security risks posed by the continued efforts of countries of concern to access, exploit, and weaponize Americans' bulk sensitive personal and U.S. government-related data. This rule reflects the Department's careful consideration of the comments received in response to the March 5, 2024 Advance Notice of Proposed Rulemaking (ANPRM) and the October 29, 2024 Notice of Proposed Rulemaking (NPRM) as well as feedback from hundreds of representatives from companies and organizations and extensive consultation with dozens of other U.S. Government agencies and offices, along with engagement foreign partners. As previewed in the ANPRM and NPRM, the final rule establishes a national-security program within the Justice Department's National Security Division that restricts and in some instances prohibits U.S. persons from engaging in certain categories of data transactions with six "countries of concern" (including covered persons and entities subject to coercion by those countries) because such transactions pose unacceptable national-security risks of giving those countries, entities, or persons access to U.S. bulk sensitive personal data or government-related data.

The rule issued today will become effective 90 days after publication. Certain affirmative compliance obligations will be phased in with a later effective date of 270 days after publication. The Department also intends to continue engaging with industry and other stakeholders to determine whether any general licenses are appropriate as this program goes into effect. The Department also anticipates issuing public guidance on compliance with, and enforcement of, the rule before its effective date.

This fact sheet offers a concise summary of the final rule and outlines the timeframe for its implementation. For specific details, please refer to the final rule in the Federal Register (which will be codified at 28 C.F.R. Part 202).

Background

Americans generate a vast digital footprint that, without protective measures, countries of concern can weaponize to threaten our national security. These countries of concern can purchase or access American's bulk sensitive personal data or government-related data through various commercial transactions and relationships. They use biometric, human 'omic, health, financial, and precise geolocation data, along with certain personal identifiers, to analyze Americans' lifestyles, spending habits, financial issues, preferences, and personal visits to sensitive locations like places of worship,

government facilities, and health clinics. Countries of concern use this data for cyber-attacks, blackmail, espionage, and intimidating activists, academics, political figures, and journalists, as well as enhancing military capabilities and for other malicious activities. Countries of concern employ advanced technologies like big-data analytics, artificial intelligence (AI), and high-performance computing to manipulate and exploit this data more effectively. Before the issuance of this final rule, existing laws failed to fully protect against these national security risks, permitting countries of concern access to such sensitive data through commercial means.

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

Executive Order and The Final Rule

On February 28, 2024, acting pursuant to the International Emergency Economic Powers Act (IEEPA), which vests the President with authority to deal with extraordinary threats to national security and foreign policy that have their source in whole or in part outside the United States, President Biden issued Executive Order 14117, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" (E.O.). The E.O. expanded the national emergency declared in Executive Order 13873 (2019) to address threats from foreign adversaries to U.S. information and communications technology and supply chains, and broadened efforts to protect sensitive data as outlined in Executive Order 14034, "Protecting Americans' Sensitive Data From Foreign Adversaries" (2021). The E.O. directed the Department to establish and implement regulations to address the threat from certain countries of concern

attempting to access and exploit bulk amounts of U.S. sensitive personal data and U.S. Government-related data. Earlier this year, the Department released an ANPRM with a 45-day public comment period and an NPRM with a 31-day public comment period. The Department received approximately 140 comments in total on the ANPRM and NPRM, and engaged with hundreds of stakeholders representing thousands of companies and organizations to solicit feedback.

As previewed in the ANPRM and the NPRM, the final rule restricts and in some cases prohibits U.S. persons from engaging in certain classes of transactions that pose an unacceptable risk of giving countries of concern or covered persons access to U.S. bulk sensitive personal data and U.S. government-related data. Among other things, the final rule identifies certain classes of prohibited, restricted, and exempt transactions; identifies countries of concern and covered persons to which the prohibitions and restrictions apply; establishes processes for licensing and advisory opinions; defines terms and sets bulk thresholds for triggering the rule's prohibitions and restrictions on covered data transactions involving bulk sensitive personal data; addresses recordkeeping, auditing reporting, and other compliance requirements; and establishes enforcement mechanisms that include civil and criminal penalties.

Overview

The final rule closely tracks the NPRM but adjusts certain deadlines, thresholds, and definitions in response to comments and stakeholder engagement.

Countries of Concern: As previewed in the ANPRM and NPRM, the final rule designates six countries—China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela—as countries of concern because they have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or the security and safety of U.S. persons, and because they pose a significant risk of exploiting bulk U.S. sensitive personal and government-related data.

Covered Persons: The final rule preserves the scope of the definition of covered persons in the NPRM, but amends the language to align more closely with the Department of the Treasury's Office of Foreign Assets Control's (OFAC) analogous 50-percent rule, and ensure entities 50 percent or more owned by a covered person are considered covered persons. The rule primarily defines four classes of covered persons: (1) foreign entities that are 50 percent or more owned by a country of concern, organized under the laws of a country of concern, or have their principal place of business in a country of concern; (2) foreign entities that are 50 percent or more owned by a covered person; (3) foreign employees or contractors of countries of concern or entities that are covered persons; and (4) foreign individuals primarily resident in countries of concern.

As previewed in the ANPRM and NPRM, these four classes are supplemented by a public list of individuals and entities designated by the Department as covered persons. Under the rule, the Department can also designate any person, regardless of location, that it determines to be, or to have been, controlled by or under the jurisdiction of a country of concern or a covered person, or who acts, has acted, or is likely to act on behalf of such entities, or who knowingly causes or is likely to cause a violation of this part, as a covered person.

Sensitive Personal Data: As previewed in the ANPRM and NPRM, the final rule regulates transactions involving six categories of sensitive personal data that a country of concern or covered person could exploit to harm U.S. national security if that data is linked or linkable to any identifiable U.S. individual or to a discrete and identifiable group of U.S. persons. These six

categories are: (1) certain covered personal identifiers (e.g., names linked to device identifiers, social security numbers, driver's license, or other government identification numbers); (2) precise geolocation data (e.g., GPS coordinates); (3) biometric identifiers (e.g., facial images, voice prints and patterns, and retina scans); (4) human genomic data and three other types of human 'omic data (epigenomic, proteomic, or transcriptomic); (5) personal health data (e.g., height, weight, vital signs, symptoms, test results, diagnosis, digital dental records, and psychological diagnostics); and (6) personal financial data (e.g., information related to an individual's credit, debit cards, bank accounts, and financial liabilities, including payment history).

As previewed in the ANPRM and NPRM, the final rule categorically excludes certain categories of data from the definition of the term "sensitive personal data," such as public or nonpublic data that do not relate to an individual (e.g., trade secrets and proprietary information), data that is already lawfully publicly available from government records or widely distributed media, and personal communications and certain informational materials. These exclusions apply to each of the categories of sensitive data.

Bulk Sensitive Personal Data Thresholds and U.S. Government-Related Data: As previewed by the ANPRM and NPRM, the final rule's prohibitions and restrictions generally apply to covered data transactions involving sensitive personal data that exceeds certain bulk volume thresholds. "Bulk" refers to any amount of sensitive personal data, whether the data is anonymized, pseudonymized, de-identified, or encrypted, that exceeds certain thresholds in the aggregate over the preceding 12 months before a "covered data transaction." The rule establishes the following bulk thresholds:

- human genomic data on over 100 U.S. persons, and the three other covered categories of human 'omic data on over 1,000 U.S. persons,
- biometric identifiers on over 1,000 U.S. persons,
- precise geolocation data on over 1,000 U.S. devices,
- personal health data and personal financial data on over 10,000 U.S. persons,
- certain covered personal identifiers on over 100,000 U.S. persons, or
- any combination of these data types that meets the lowest threshold for any category in the dataset.

As the final rule details, the Department based these thresholds on an extensive risk-based analysis, taking into account the threats, vulnerabilities, and consequences associated with the human-centric and machine-centric characteristics of each type of data.

As the ANPRM and NPRM previewed, these bulk thresholds do not apply to transactions involving certain government-related data, which are regulated regardless of the volume. The final rule defines two categories of government-related data. With respect to data on the locations of government activities, the rule treats any precise geolocation data within geographic areas listed on the Department's public Government-Related Location Data List as government-related data. In determining whether to add a geographic area to a list, the Department will consult with agency partners to determine whether precise geolocation data about the area poses a heightened risk of being exploited by a country of concern to reveal insights about federal government-controlled locations, which could harm national security. With respect to data on U.S. Government personnel,

the final rule treats any sensitive personal data marketed as linked to current or recent former U.S. Government employees or contractors (including the military and intelligence community) as government-related data.

Prohibitions and Restrictions: As previewed in the ANPRM and NPRM, the final rule identifies categories of covered data transactions involving access by countries of concern or covered persons to bulk sensitive personal data or government-related data that U.S. persons are prohibited or restricted from engaging in with countries of concern or covered persons.

- The two categories of **prohibited transactions** are data brokerage and covered data transactions involving access to bulk human 'omic data or human biospecimens from which such data can be derived. The final rule defines human 'omic data as human genomic, human epigenomic, human proteomic, and human transcriptomic data.
- The three categories of **restricted transactions** are vendor, employment, and non-passive investment agreements. These restricted transactions with countries of concern or covered persons are permitted if they meet certain security requirements developed by the Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA) that seek to mitigate the risk of access by countries of concern or covered persons to bulk U.S. sensitive personal data or government-related data involved in the transactions. CISA is concurrently publishing its security requirements. These security requirements include, but are not limited to, cybersecurity measures such as basic organizational cybersecurity policies and practices, physical and logical access controls, data masking and minimization, encryption, and the use of privacy-enhancing techniques. The final rule includes a technical correction to the definition of "access" (§ 202.201) to prevent inadvertently treating restricted transactions that comply with CISA's security requirements by denying access as outside the scope of the rule.
- The rule addresses the risk of data being **resold or transferred through third parties** to countries of concern or covered persons by requiring U.S. persons engaged in data brokerage with any foreign person that is not a covered person to satisfy certain conditions, including, but not limited to, contractually requiring that the foreign person refrain from reselling or providing access to that data to a country of concern or covered person through a subsequent covered data transaction. The Department anticipates that forthcoming compliance and enforcement guidance will provide model contractual language to satisfy this requirement.
- To address potential **circumvention** of the regulations, the rule prohibits U.S. persons from knowingly directing any covered data transaction that is prohibited if conducted by a U.S. person. The rule also prohibits transactions designed to evade the regulations, those that cause or attempt to cause a violation of the regulations, and conspiracies to violate the regulations. The final rule clarifies that U.S. persons providing third-party platforms or infrastructure are not civilly or criminally responsible for their customers' prohibited or restricted transactions on those platforms. They are only responsible for the prohibited or restricted transactions in which they themselves conduct.

Exempt Transactions: As previewed in the ANPRM and NPRM, the final rule exempts certain classes of data transactions. Building on the specific exemptions previewed in the ANPRM and NPRM, and based on helpful feedback from commenters and stakeholders during the Department's engagements, the final rule exempts:

1. **Personal communications** that do not transfer anything of value; the import or export of **informational materials** involving expressive materials; and **travel** information, including data about personal baggage, living expenses, and travel arrangements.
2. **Official U.S. Government activities**.
3. **Financial services** if they involve transactions ordinarily incident to and part of providing financial services, such as banking, capital markets, futures or derivatives, or financial insurance services; financial activities authorized for national banks; activities defined as financial in nature or complementary to a financial activity under the Bank Holding Company Act; transfer of personal financial data incidental to e-commerce; and the provision of investment management services that provide advice on portfolios or assets for compensation, including related ancillary services.
4. **Corporate group transactions** between a U.S. person and its foreign subsidiary or affiliate, if they are ordinarily incident to and part of routine administrative or business operations, such as human resources, payroll, taxes, permits, compliance, risk management, travel, and customer support.
5. **Transactions required or authorized by Federal law or international agreements**, which include agreements such as the Convention on International Civil Aviation (2022);the WHO constitution (1946); various U.S.-China agreements on customs, legal assistance, and taxation; the U.S.-Cuba Extradition Treaty (1905), U.S.-Russia agreements on customs (1994) and legal assistance (1999), the U.S.-Venezuela Legal Assistance Treaty (1997), the International Health Regulations (2005), and certain public health surveillance and response mechanisms. Additionally, transactions are exempt to the extent they are ordinarily incident to and part of compliance with federal law and regulations.
6. **Investment agreements** after they have become subject to certain mitigation or other action taken by the Committee on Foreign Investment in the United States (CFIUS), if CFIUS explicitly designates them as exempt.
7. Transactions that are ordinarily incident to and part of the provision of **telecommunications services**, including all voice and data communications services regardless of format or mode of delivery, including communications services delivered over cable, Internet Protocol, wireless, fiber, or other transmission mechanisms, as well as arrangements for network interconnection, transport, messaging, routing, or international voice, text, and data roaming.
8. Data transactions with countries of concern or covered persons involving **drug, biological product, device, or combination product approvals or authorizations** if the data transactions involve "regulatory approval data" necessary to obtain or maintain regulatory approval. "Regulatory approval data" means sensitive personal data that is de-identified or pseudonymized consistent with FDA regulations (21 C.F.R. 314.80(i)) and required by a regulatory entity to research or market a drug, biological product, device, or combination product, including post-marketing studies and surveillance. It excludes data not reasonably necessary for assessing safety and effectiveness. The terms "drug," "biological product," "device," and "combination product" have the meanings set forth in 21 U.S.C. § 321(g)(1), 42 U.S.C. § 262(i)(1), 21 U.S.C. § 321(h)(1), and 21 CFR § 3.2(e).
9. **Other clinical investigations and post-marketing surveillance data** if the transactions are part of clinical investigations regulated by the FDA under sections 505(i) and 520(g) of the Federal Food, Drug, and Cosmetic Act, or support FDA applications for research or marketing permits for drugs, biological products, devices, combination products, or infant formula, and the data are de-identified or pseudonymized consistent with FDA regulations (21 C.F.R. 314.80(i)). They are also exempt if they are part of the collection or processing

of clinical care data indicating real-world performance or safety of products, or post-marketing surveillance data necessary to support or maintain FDA authorization, provided the data is de-identified or pseudonymized.

The final rule also carves out transactions data that is lawfully publicly available from government records or widely distributed media (like freely available, open-access repositories), and metadata that is ordinarily associated with expressive materials, or that is reasonably necessary to enable the transmission or dissemination of expressive materials (such as geolocation data embedded in digital photographs).

Licensing: As previewed in the ANPRM and NPRM, the final rule authorizes the Department to issue general licenses to authorize certain categories of otherwise prohibited or restricted transactions under specified conditions. Transactions meeting these conditions will not require further authorization and could, for example, ease sector-specific transactions by authorizing orderly wind-down conditions for covered data transactions. As also previewed in the ANPRM and NPRM, the rule authorizes the Department to issue specific licenses for specific transactions by parties who apply for and disclose details of their intended transactions in a license application to the Department. The rule sets out the requirements and procedures for the issuance of general and specific licenses, including the process to apply for a specific license or seek reconsideration of a denied license based on new information. The Department intends to issue separate instructions on how to apply for a specific license.

Guidance and Advisory Opinions: As previewed in the ANPRM and NPRM, the final rule permits the Department to issue general public guidance to address frequently asked questions and common issues, as well as advisory opinions to address the applicability of the regulations to specific transactions. The rule permits regulated parties to request advisory opinions about the interpretation and application of the regulations to actual specific transactions, not hypothetical situations.

Compliance Obligations: As previewed in the ANPRM and NPRM, the final rule does not prescribe general due-diligence, recordkeeping, reporting, or other compliance requirements across the U.S. economy or across all data transactions. Instead, like compliance under economic-sanctions programs administered by OFAC, U.S. companies and individuals are expected to develop and implement compliance programs based on their individualized risk profiles. These risk-based compliance programs 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. If a violation occurs, the Department will consider the adequacy of the compliance program in any enforcement action.

As also previewed in the ANPRM and NPRM, the final rule establishes affirmative compliance obligations only as conditions for U.S. persons engaged in a restricted transaction. These affirmative compliance obligations for restricted transactions include implementing a comprehensive compliance program, which would include implementing risk-based procedures to verify and log data flows, sensitive personal and government-related data types and volume, transaction parties' identities, data end-use and transfer methods, and vendor identities. These conditions also include establishing written policies on data security and compliance that are certified annually by a responsible officer or employee, conducting and retaining the results of an annual audit by an internal or external independent auditor to verify compliance with the security requirements

established by CISA, and maintaining and certifying the accuracy of records for 10 years documenting data transfer methods, transaction dates, agreements, licenses, advisory opinions, and any relevant documentation received or created in connection with the transactions.

Reporting Requirements: As previewed in the ANPRM and NPRM, the final rule establishes certain reporting requirements to ensure compliance with these rules and safeguard national security, including:

- Annual reports filed by U.S. persons engaged in restricted transactions involving cloud-computing services, if they are 25 percent or more owned, directly or indirectly, by a country of concern or covered person;
- Reports by any U.S. person that has received and affirmatively rejected an offer from another person to engage in a prohibited transaction involving data brokerage;
- Reports by U.S. persons engaged in a covered data transaction involving data brokerage with a foreign non-covered person if the U.S. person knows or suspects that the foreign counterparty is violating the restrictions on resale and onward transfer to countries of concern or covered persons; and
- Reports by U.S. persons invoking the exemption for certain data transactions that are necessary to obtain or maintain regulatory approval to market a drug, biological product, device, or a combination product in a country of concern.

The final rule allows companies to use existing audits, reports, and other compliance practices as long as they meet the requirements of this rule, and thus there is no need to create duplicative or separate systems or reports. The final rule also clarifies that U.S. persons may use either internal or external audits so long as they are independent and meet the other requirements of the rule. The final rule further clarifies that audits for restricted transactions need only examine a U.S. person's restricted transactions (not all data transactions) and only relevant (not all) policies, personnel, and systems.

Enforcement: Similar to other IEEPA-based programs, the final rule permits the Department to conduct investigations, hold hearings, examine and depose witnesses, and issue subpoenas for witnesses and documents related to any matter under investigation. Violations can result in civil and criminal penalties. Civil penalties, which are subject to the Federal Civil Penalties Inflation Act, can be up to $368,136 or twice the amount of the transaction involved, whichever amount is greater. The rule establishes the processes for the Department to issue findings of violations and civil penalties, including an opportunity for parties to respond before the Department issues a penalty. Willful violations can lead to criminal fines up to one million dollars ($1,000,000) and up to 20 years' imprisonment.

Frequently Asked Questions

When does the final rule go into effect?

- The rule becomes effective 90 days after publication in the Federal Register. The affirmative due diligence and audit requirements for restricted transactions (in subpart J of the rule) and certain reporting requirements for restricted transactions (in §§ 202.1103 and 202.1104 of the rule) will be phased-in and will not become effective until 270 days after the rule's publication in the Federal Register. The Department intends to continue to engage with companies and

stakeholders to determine whether any wind-down or other general licenses are appropriate.

- The prohibitions and restrictions of the rule will apply to all covered data transactions initiated, pending, or completed on or after the relevant effective date. Unless exempt or otherwise authorized, on or after the relevant effective date, U.S. persons knowingly engaging in a prohibited or restricted covered data transaction are expected to comply with the rule, notwithstanding any contract entered into or any license or permit granted before the effective date.

Once in effect, who must comply with the final rule?

- All U.S. persons (to include entities organized under the laws of the United States as defined in the rule) must comply with the final rule when it becomes effective. Non-U.S. persons will also be subject to certain prohibitions of the final rule. For example, non-U.S. persons are prohibited from causing or conspiring to cause U.S. persons to violate the final rule and are prohibited from engaging in transactions that have the purpose of evading the final rule. More broadly, the Department anticipates sharing compliance, enforcement, and other guidance before the rule becomes effective.

What part of the Department is responsible for implementing this authority?

- This program is housed in the Department's National Security Division, and its Foreign Investment Review Section (FIRS) will implement this authority on a day-to-day basis, working closely with other Department components as appropriate and in coordination with the Department of Homeland Security and other agencies.

Does the final rule ban apps or social-media platforms sourced from foreign adversaries?

- No. The final rule does not ban apps or social-media platforms, nor does it concern any single app or technology. The final rule addresses only the most serious data-security risks (not all national-security risks, such as application security or disinformation) posed by only a subset of the data collected and used by apps and social-media platforms (sensitive personal data, not all data), and only with respect to a limited number of identified countries of concern. Furthermore, the final rule addresses only the national security risks of giving covered persons or countries of concern access to this data—not the broader domestic privacy challenges posed by social media. The final rule excludes the regulation of transactions to the extent they involve expressive information under 50 U.S.C. § 1702(b)(3), such as videos, artwork, and publications.

Does the final rule regulate the domestic collection, processing, and use of data in the United States?

- No. The final rule does not regulate purely domestic transactions between U.S. persons—such as the collection, maintenance, processing, or use of data by U.S. persons within the United States—except to the extent that such U.S. persons are affirmatively and publicly designated as covered persons.

Does this final rule give the Department new surveillance authorities or the ability to track Americans' data?

- No. The final rule has nothing to do with the U.S. Government's authorities to lawfully engage in law-enforcement and national-security activities to gather intelligence. Nothing in the rule, on its face or in practice, requires U.S. companies to surveil their employees,

customers, or other private entities. Personal communications, expressive information, and metadata ordinarily associated with expressive materials (or that is reasonably necessary to enable the transmission or dissemination of expressive materials) are categorically excluded from the scope of the rule. And the rule does not regulate purely domestic transactions between U.S. persons, like the collection, maintenance, processing, or use of data by U.S. persons within the United States (unless one of those persons is a designated covered person).

Does this final rule stop the sharing of data for medical, health, or science research or the development and marketing of new drugs?

- No. The final rule prohibits and restricts only certain categories of commercial transactions that involve the exchange of payment or other consideration and meet other criteria. The final rule does not prohibit or restrict U.S. research in countries of concern, or U.S. research partnerships or collaborations with countries of concern or covered persons, that do not involve the exchange of payment or other consideration as part of a commercial transaction. In addition, the rule contains exemptions meant to preserve critical health research, including exemptions for federally funded research, for sharing data pursuant to international agreements (including certain pandemic-related and global-health-surveillance agreements), for submissions of regulatory approval data for medical drugs, devices, and biological products, and for certain clinical-investigation data and post-marketing surveillance data.

Who can I contact for more information?

- For press inquiries, please contact DOJ's Office of Public Affairs here. For non-press inquiries about the final rule and the implementation of this program, please email nsd.firs.datasecurity@usdoj.gov. For more information, please see the Foreign Investment Review Section's website.