Paul | Weiss

2024 YEAR IN REVIEW

CFIUS, Outbound Investments and Export Controls

Paul, Weiss, Rifkind, Wharton & Garrison LLP

December 6, 2024

2024 Year in Review: CFIUS, Outbound Investments and Export Controls

In the past year, the U.S. government's efforts to counter China led to a number of noteworthy regulatory developments. The past months in particular have seen a flurry of activity, as the outgoing Biden administration has finalized initiatives related to the Committee on Foreign Investment in the United States ("CFIUS" or the "Committee"), U.S. outbound investment restrictions and export controls. In this client memorandum, we explore these developments and provide key takeaways for transaction parties. Looking ahead to 2025, we expect President-elect Trump's administration will continue, and likely expand upon, the Biden administration's China-related national security initiatives, including CFIUS's continued focus on enforcement, the use of export controls as a key tool to mitigate access to critical, defense-related technologies, and the implementation and enforcement of the imminent Outbound Investment Security Program.

2024's Key Takeaways

- Despite a slight decline in overall filings, CFIUS remains a robust regulatory program reviewing hundreds of transactions a year, and the Committee has continued its transformation into a highly resourced and significant regulator of foreign investment into the United States. The decline in total filings may in part be due to increased familiarity with the regime and a shift in decision-making by transaction parties that are balancing the desire for regulatory certainty with timing risks. The decline also tracks with overall M&A trends year over year.[1]

- CFIUS expanded its enforcement activities, including by disclosing a substantial uptick in its use of monetary penalties for non-compliance with mitigation agreements (including a $60 million penalty in one case) and by issuing new regulations that enhanced its enforcement capabilities.

- The U.S. government continues to prioritize export control authorities as a critical component of its efforts to counter nation-state foreign adversaries seeking to obtain access to the United States' most sensitive technologies. In practice this has meant new, more restrictive controls on emerging technologies and increased enforcement by the U.S. government and, consequently, increased compliance and diligence considerations for companies.

- The Outbound Investment Review Program, which comes into effect January 2, 2025, will prohibit certain investments by U.S. persons in individuals or entities associated with China (including Hong Kong and Macau) involving critical national security technologies and products while requiring notification of others. Although similar in some regards to existing sanctions programs, the new outbound program represents a significant new step in that it restricts activities across categories of technologies rather than just with specifically identified parties or individuals. As discussed in greater detail below, we expect that the current categories, which are relatively tailored, may be expanded in the coming years.

[1] *See* Paul, Weiss, *M&A at a Glance (2023 Year-End Roundup)* (Jan. 16, 2024), available here.

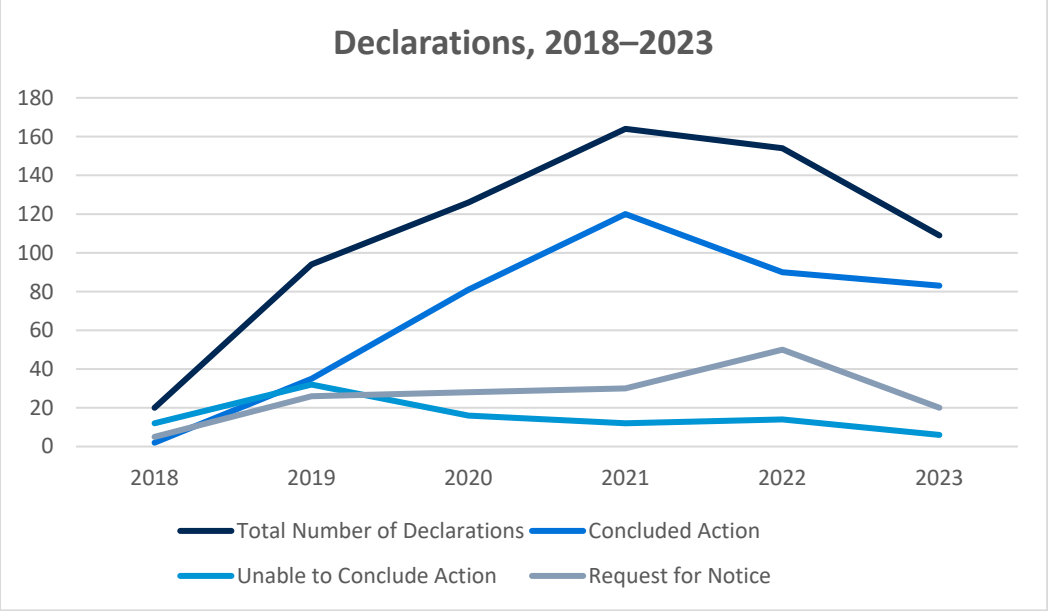
1. U.S. Inbound Investment – the Committee on Foreign Investment in the United States

2024 proved to be another momentous year for CFIUS, with the Committee expanding its jurisdiction over real estate transactions and enhancing its enforcement authorities and penalties. CFIUS also took noteworthy and precedent-setting actions this year, including the first-ever unwinding of a real estate transaction and the issuance of monetary penalties that far exceed – in both number and dollar value – the relatively limited penalties issued by CFIUS in the past.

CFIUS Transaction Reviews

CFIUS publishes annual statistics for the preceding calendar year approximately each summer and, in July 2024, issued its 2023 annual report (the "Annual Report").[2] The report provided a few noteworthy takeaways and insights:

- **Evolution of the Declaration Program**. The "declaration" filing option allows parties to make a short-form filing and potentially obtain CFIUS approval on an accelerated, 30-day timeline. But declarations have historically also carried risk: CFIUS may ask the parties to submit a full notice after reviewing the declaration, essentially sending the parties back to square one. This is a not an infrequent outcome – CFIUS has asked for a notice following review of a declaration in roughly one quarter of all declaration filings. However, CFIUS has now processed hundreds of declaration filings since the filing option became available and the vast majority of declarations are cleared in their 30-day review period. This means that, in the right circumstances, the declaration is a viable filing option. Given the complexities around the declaration process and the potential reward/risk associated with its rapid timeline, parties should consult with CFIUS counsel before choosing it.



- **A Mixed-Bag on Timing**. On the one hand, the Annual Report reflects improved efficiency in year-over-year metrics compared to the preceding year, and Treasury indicated at a recent year-end conference that it expects these improvements to continue to be reflected in the 2024 statistics, when published. On the other hand, timelines still remain somewhat elevated compared to those achieved in some of CFIUS's most efficient years. For example, the rate of transactions going into a second stage review in 2023 (54%) remains well above the percentage of second-stage reviews in 2021 (47%). Additionally, in 2023, 25% of notices were withdrawn after commencement of investigation, representing only a relatively modest improvement over the 31% of withdrawn notices in 2022, and still above historical figures. Even if a

[2] *See* Paul, Weiss, *CFIUS Releases 2023 Annual Report, Highlighting Enforcement Activity* (Aug. 14, 2024), available here; *see also* U.S. Dep't of Treasury, *Committee on Foreign Investment in the United States: Annual Report to Congress* (Jul. 23, 2024), available here ("2023 Year in Review").

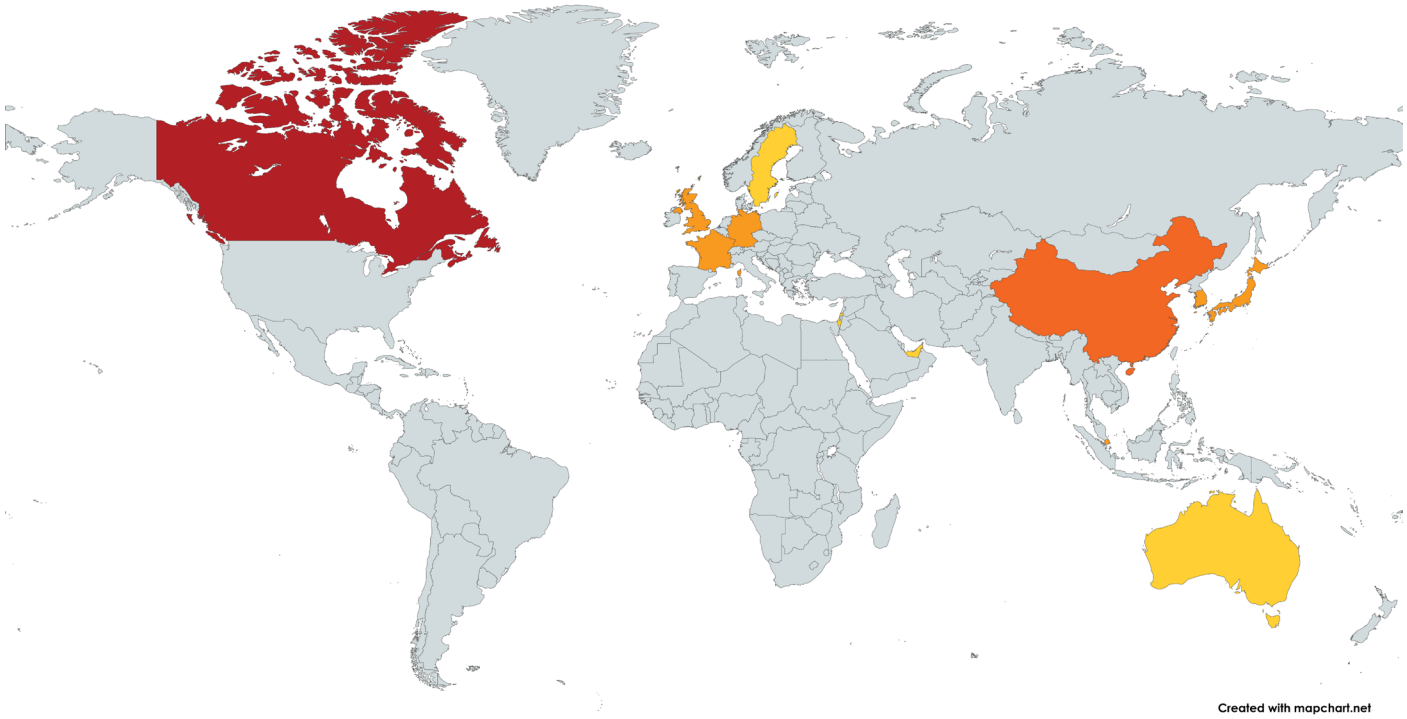
withdrawn filing is refiled and ultimately cleared, this indicates that parties encounter a very extended process in a sizeable number of transactions.

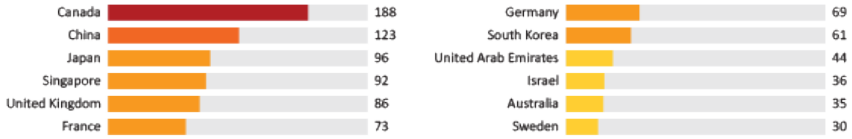
Undoubtedly, CFIUS became more efficient in 2023 than it was in 2022, and practitioners and it is welcome news that these gains were maintained, or perhaps even improved upon, in 2024. Importantly, though, many filings still face long reviews: less than half of all notice filings are cleared in the first 45 days, and almost a quarter are withdrawn after 90 days. This means that, for many transactions, long reviews still persist.

- **Mitigation Efforts and Abandoned Transactions**. In 2023, a little over one in five transactions reviewed by CFIUS required some form of mitigation as a condition to approval, and nine transactions were abandoned after CFIUS found that no mitigation would be sufficient to allow approval. Another five transactions were called off for other unspecified reasons, which could have included timing issues associated with a failure to reach agreement on mitigation. This means that, continuing with post-FIRRMA trends, mitigation is a frequent outcome for transactions and, further, that CFIUS is not afraid to conclude it cannot approve a transaction even if the parties propose mitigations. Treasury has indicated that CFIUS now monitors over 200 mitigation agreements. Careful understanding of potential mitigation outcomes is thus a critical component of the CFIUS diligence process.

- **High Risk Investments**. While Chinese investments are still high, the total filing numbers from China have steadily tapered in the last three years, and such investments appear likely to continue to be high risk, particularly those involving any of the "TID U.S. Business" categories: critical technology, sensitive personal data or critical infrastructure. That said, CFIUS's annual reports reflect that some Chinese-origin transactions are approved – these likely involve businesses that present no relevance to U.S. national security. Notably, as Chinese investments have declined, mitigation, as described above, has continued to be prevalent. This reflects that CFIUS has expanded its focus to mitigate risks associated with transactions involving U.S. allies, such as Singapore and several Middle Eastern countries.

Declarations / Notices by Home Country or Economy (30+), 2021–2023





Foreign Acquirers of U.S. Critical Tech in 2023 (5+)

CFIUS Real Estate Authorities

Until this past year, CFIUS's real estate transaction authority has not garnered significant attention – in part because all real estate transactions are subject only to voluntary filings, and also because, even where geographical considerations are at play for CFIUS, the Committee has often been able to act under its primary authority for transactions involving U.S. businesses. But this year proved noteworthy in the real estate space, as CFIUS expanded its geographic jurisdiction and effected a first-of-its-kind unwinding of a real estate transaction.[3]

In November 2024, Treasury issued a final rule expanding CFIUS's jurisdiction over real estate transactions.[4] The rule brings 40 new military installations under CFIUS's one-mile radius jurisdiction and 19 new military installations under its 100-mile radius jurisdiction, and moves an additional eight military installations from its one-mile radius jurisdiction to its 100-mile radius jurisdiction (effectively expanding the zone of properties subject to potential review in relation to these sites). This is the single largest expansion of CFIUS's real estate jurisdiction since FIRRMA was implemented, and now brings the total number of listed installations to over 225.

Of even greater importance, 2024 saw the first ever use of CFIUS's real estate authority to unwind a transaction. In May 2024, President Biden ordered a Chinese-owned crypto company to divest real estate it owned that was within one mile of a U.S. strategic missile base in Cheyenne, Wyoming.[5] The order followed a "non-notified" review by CFIUS, which received a tip about the transaction from a member of the public.

The prohibition is noteworthy for a few reasons. First, it is to date the only divestment of property under CFIUS's real estate authorities. Second, CFIUS specifically emphasized that it was acting based on a public tip, demonstrating that the Committee's robust "non-notified" review process leverages a broad array of information sources, including the collection and analysis of public tips. Third, in a corresponding press release, Treasury said, "CFIUS expects complete, accurate, and timely information." This suggests that CFIUS's actions may have been prompted at least in part by the divested company's unresponsiveness or inaccurate answers, which signifies the Committee is willing to act aggressively when faced with untimely engagement.

CFIUS Enforcement

CFIUS currently monitors well over two hundred active mitigation agreements and, with the advent of FIRRMA's mandatory filing program, is now charged with identifying transactions that failed to make mandatory filings. In recent years, CFIUS has publicly emphasized its focus on enforcement, for example, issuing enforcement and penalty guidelines in 2022. In 2024, however, CFIUS backed up that enforcement talk with concrete actions.

- **Enforcement Actions and Methodologies**. Treasury unveiled a new enforcement website in August 2024.[6] The website details specific enforcement actions that CFIUS has undertaken in recent years. These disclosures depict a dramatic expansion in CFIUS's enforcement activities and are notable in their own right – until the creation of this website, CFIUS had shared very little detail about specific enforcement actions. Six of the eight enforcement actions described on the website are from 2023–2024. In 2023 and 2024, to date, CFIUS issued three times more penalties than CFIUS had in its entire 50-

3 *See* Paul, Weiss, *President Biden Orders Chinese Crypto Company to Divest Real Estate in Close Proximity to U.S, Missile Base* (May 22, 2024), available here.

4 *See* 31 C.F.R. Part 802.

5 The White House, *Order Regarding the Acquisition of Certain Real Property of Cheyenne Leads by MineOne Cloud Computing Investment I L.P.* (May 13, 2024), available here.

6 U.S. Dep't of Treasury, *CFIUS Enforcement*, available here.

year history.[7] One penalty amounted to $60 million, demonstrating that not only is CFIUS willing to penalize more frequently, it is willing to assess substantially large fines.

The website also notes that in a number of instances, CFIUS made formal determinations of violations that it concluded did not warrant a monetary penalty – calling these "Determination of Noncompliance Transmittal" (or "DONT") Letters. Treasury explained that its conclusions not to assess a monetary penalty are based on relevant mitigating factors, including whether it was a first-time violation, inadvertency, and/or otherwise limited in scope and/or having a potential effect on national security. Although not including a monetary penalty, DONT Letters are nonetheless significant, as parties could be required to disclose them in diligence processes and other contexts.

- **Expanded Enforcement Authorities**. In November 2024, Treasury issued a final rule augmenting the penalty and enforcement authorities of CFIUS.[8] Key parts of the rule include:

  - Increased Penalties: The final rule expands the circumstances in which a civil monetary penalty may be imposed due to a party's material misstatement and omission and increases the maximum civil penalty from $250,000 per violation to $5,000,000 (or in some cases the value of the transaction) for material misstatements or omissions in declarations and notices; for the failure to submit a mandatory declaration, and for violations of material provisions of mitigation agreements, mitigation conditions imposed by CFIUS, or orders issued by CFIUS.

  - Information Collection Authorities: First, the final rule expands the types of information CFIUS can require parties to submit related to "non-notified transactions." Second, the final rule expressly obligates parties to respond to requests for information relating to monitoring for compliance with or enforcing the terms of a mitigation agreement, order, or condition, as well as information to determine whether parties made material misstatements or omissions. Third, the final rule lowers the threshold for the Committee's use of subpoena power from when it is "deemed necessary" to when it is "deemed appropriate." The threshold change of CFIUS's subpoena power could be significant in terms of the Committee's efforts to procure information from parties.

  - Transaction Review: The final rule explains that in order for CFIUS to complete an investigation of a transaction within the time prescribed by statute, the parties must respond to its proposals of terms to mitigate national security risks in a timely manner, and therefore imposes an extendable three-day period for parties to submit substantive responses to proposed mitigation terms. This is a significant change to CFIUS's practice which currently allows parties to take substantial amounts of time to review and negotiate mitigation proposals from the Committee, particularly in cases where a transaction had not yet closed and where closing was conditioned on clearance from CFIUS.

2. Outbound Investment – Treasury's new Outbound Investment Security Program

One of the most notable regulatory developments in the past year is Treasury's implementation of President Biden's August 2023 Executive Order on "Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern."[9]

---

7 U.S. Dep't of Treasury, *Treasury Unveils New CFIUS Enforcement Website to Provide Further Clarity and Transparency Regarding CFIUS Penalties and Other Enforcement Actions* (Aug. 14, 2024), available here.

8 *See* Note 7.

9 The White House, *Executive Order on Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern* (Aug. 9, 2023), available here.

Treasury's final rule, issued in October 2024 and effective January 2, 2025, either prohibits or requires notification regarding certain ***investments by U.S. persons***[10] ***in covered foreign persons***, i.e., individuals or entities associated with a country of concern (presently China, Hong Kong, and Macau) that are ***engaged in covered activities*** (e.g., research, development, or manufacturing) involving ***covered national security technologies and products*** (i.e., semiconductors and microelectronics, quantum information technologies, and AI systems).

- **Covered Transactions**. In addition to requiring the involvement of a covered foreign person, covered activity, and covered technology or product, the final rule applies only to certain transaction types. The categories are quite broad and include (1) the acquisition of an equity interest or contingent equity interest in a person that the U.S. person knows at the time of the acquisition is a covered foreign person; (2) provision of a loan or similar debt financing arrangement to a person that the U.S. person knows at the time of the provision if a covered foreign person; and (3) conversion of a contingent equity interest into an equity interest in a person that the U.S. person knows at the time of the conversion is a covered foreign person. The final rule also covers additional transactions types, including greenfield investments or other related expansion, entrance into a joint venture, and acquisitions of a limited partner or equivalent ("LP") interest in a non-U.S. person pooled investment fund.

  There are, however, certain excepted categories of transactions that can be engaged in even if a covered person, activity, and technology is involved. The primary exemptions include: (1) publicly traded securities, (2) certain LP investments, (3) derivatives, (4) buyouts of a country of concern, (5) intracompany transactions, (6) certain pre-final rule binding commitments, (7) certain syndicated debt financings, (8) equity-based compensation, and (9) third-country measures.

  - Those that wish to take advantage of the excepted categories should review the final rule in close detail, as many of these exceptions are crafted narrowly and thus may be more limited than they appear. For example, LP investments have a number of conditions that limit the applicability of the exception, including an investment cap.

- **What Is Prohibited and What Requires Notification**.

  The final rule has detailed provisions that define the relevant terms, including what constitutes a U.S. person, who is a covered foreign person, what types of activities are covered and what types of technologies are covered. We strongly encourage careful scrutiny of the final rule. The following table provides a brief overview delineating the types of transactions, by technology category, that are prohibited versus those subject to only notification (transactions not identified would neither by prohibited nor require notification).

Category	Prohibited	Notification Required
Semiconductors and microelectronics	Developing or producing any electronic design automation software for the design and fabrication of advanced semiconductors; designing of advanced integrated circuits; fabricating advanced integrated circuits; packaging of advanced integrated circuits; developing, installing, selling or producing any supercomputer enabled by advanced integrated circuits.	Designing, fabricating or packaging of integrated circuits that are not otherwise prohibited are subject to a notification requirement to Treasury.

[10] U.S. person is defined broadly to include any U.S. citizen or lawful permanent resident, as well as any entity organized under the laws of the United States or any jurisdiction within the United States, including foreign branches of any such entity, and any person in the United States.

Certain AI systems	Developing any AI system intended exclusively for specific end uses (specifically, military, government intelligence or mass-surveillance end uses), those trained with more than 10^25 computational operations or with biological sequence data and more than 10^24 computational operations.	Developing any AI system that is not prohibited but is either designated or intended for specific end uses or applications or trained with more than 10^23 computational operations is subject to a notification requirement to Treasury.
Quantum information technologies	Developing any quantum computers or producing any essential components necessary for creating a quantum computer, or the development or production of specific quantum sensing platforms and certain quantum networks or quantum communication systems.	None (entirely prohibited).

3. The Increasing Importance of Export Controls and Related Regimes

In 2024, export controls emerged as one of the most important components of the U.S. national security tool-kit, and one that carries significant compliance risk for U.S. companies in particular, including financial institutions. To that end, the Department of Commerce ("Commerce") and its interagency partners, engaged in a number of significant regulatory and enforcement actions, and issued new guidance during the past year with a particular focus on China. As recently as December 2, 2024, Commerce's Bureau of Industry and Security ("BIS") announced a "package of rules designed to further impair" China's capability to produce advanced semiconductors used in next-gen weapon systems and in AI, including new controls on semiconductor manufacturing equipment and related software tools and on high-bandwidth memory.[11]

- **Item-Based Controls**. Commerce has imposed increasingly restrictive item-based export controls on U.S.-origin goods, software and technology. These new controls target semiconductors and microelectronics, quantum computing, artificial intelligence, drones and encryption technologies. In recent years, BIS has also increased the amount of items (which include not only physical goods but also software and "technology" (e.g., know how, technical specifications)) that require a license to be exported to China. AI, in particular, remains an area of dynamic development in the export control space, as BIS seeks to ensure appropriate classification and protection of the fast-developing technology.

- **End-User Controls and the Entity List**. U.S. export controls also include end-user specific controls, including the "Entity List," which imposes a prohibition on listed individuals and entities from receiving specified U.S.-origin items absent a license from BIS. Hundreds of Chinese companies are on the Entity List, including major technology companies such as Huawei. On December 2, 2024 alone, BIS added 140 entities acting to further China's advanced chip goals. In recent years, Entity List designations have also become a major tool used by the U.S. government to restrict exports of higher technology U.S. origin items to specific Chinese companies or sectors of concern, but they have also more broadly become a tool of carrying out U.S. government policies in areas not directly tied to export control or technology transfer (e.g., human rights-related issues). Notably, the U.S. government demonstrated this year when it took the extremely rare step of removing a company from the Entity List that when companies change their behavior to protect U.S. national security and human rights, they can be delisted.[12]

---

11 *See* U.S. Dep't of Commerce, *Commerce Strengthens Export Controls to Restrict China's Capability to Produce Advanced Semiconductors for Military Applications* (Dec. 2, 2024), available here.

12 *See* Paul, Weiss, *Sandvine Removed From Commerce Department's Entity List Following Significant Corporate Reforms to Protect Human Rights* (Oct. 21, 2024), available here.

- **Enforcement Actions & the Disruptive Technology Strike Force**. In February 2023, the U.S. Department of Justice ("DOJ") and Commerce launched the Disruptive Technology Strike Force ("DTSF") to target illicit actors, strengthen supply chains and protect critical technological assets from being acquired or used by nation-state adversaries.[13] The activities of the DTSF have ramped up significantly, with the DTSF publicly charging 25 cases involving, among other things, sanctions and export control violations, as well as taking a number of other administrative actions. In 2024, BIS investigations convicted over 65 individuals and businesses for export violations resulting in nearly $5 million in fines, $3 million in forfeitures, over $15 million in restitution, and thousands of months of imprisonment.[14] This is in addition to the over 65 administrative export matters, which according to BIS resulted in over $6.5 million in civil penalties.

- **First Ever Use of the ICTS Rule to Issue a Final Determination**. In June 2024, BIS prohibited the U.S. subsidiary of a Russia-based anti-virus software and cybersecurity company, Kaspersky Lab Inc. ("Kaspersky"), from providing its products or services in the United States or to U.S. persons on national security pretenses.[15] This is the first time BIS's Office of Information and Communications Technology and Services ("OICTS"), whose mission is to "investigate whether certain information and communications technology or services transactions in the United States pose an undue or unacceptable national security risk," issued a Final Determination.

  OICTS's determination stems from an investigation first started by the Department of Homeland Security nearly seven years ago in 2017 when it mandated federal agencies remove and discontinue use of Kaspersky products on federal systems and a 2021 referral from DOJ requesting BIS review Kaspersky's software and related services in the United States. According to BIS, Kaspersky posed an undue or unacceptable risk to national security because it is subject to the jurisdiction, control, or direction of the Russian government, which is a "foreign adversary" that continues to threaten the United States. Moreover, BIS reasoned that Kaspersky's software provides bad actors in Russia with access to sensitive U.S. customer information, as well as presenting the capability and opportunity to install certain malicious software or withhold critical cybersecurity updates.

- **Guidance for Financial Institutions**. In October 2024, BIS issued guidance to financial institutions on "best practices" for compliance with the Export Administration Regulations ("EAR"), including General Prohibition 10,[16] which includes a prohibition on "servic[ing]" a transaction "with knowledge" that it has or will violate the EAR.[17] While General Prohibition 10 is longstanding and applies broadly to all types of entities, the traditional understanding as of several years ago was that BIS was not actively seeking to bring enforcement cases against financial institutions under it. In the Guidance, BIS recommends, among other things, that financial institutions incorporate export controls due diligence when "onboarding a new customer and as part of regular risk-based due diligence thereafter" and even engage in real-time screening for certain BIS lists. U.S. and non-U.S. financial institutions engaged in international transactions should consider reviewing which of the "best practices" described by BIS they currently follow, and what steps would be necessary to close any gaps.

---

13 U.S. Dep't of Justice, *Justice and Commerce Departments Announce Creation of Disruptive Technology Strike Force* (Feb. 16, 2023), available here.

14 U.S. Dep't of Commerce, *Don't Let This Happen to You, Actual Investigations of Export Control and Antiboycott Violations* (Nov. 2024), available here.

15 *See* Final Determination: Case No. ICTS-2021-002, Kaspersky Lab, Inc., 89 FR 52434, available here.

16 *See* Paul, Weiss, *Commerce's BIS Issues Guidance to Financial Institutions on Export Control Compliance* (Oct. 15, 2024), available here; *see also* U.S. Dep't of Commerce, *Bureau of Industry and Security Issues New Guidance to Financial Institutions on Best Practices for Compliance with the Export Administration Regulations* (Oct. 9, 2024), available here (the "Guidance"); *see also* Press Release, available here.

17 15 C.F.R. § 736.2.

4. What's to Come in 2025 – President Trump 2.0

Current CFIUS, outbound investment, and export controls regimes reflect initiatives from the first Trump administration. Using national security authorities to address the multifaceted threat posed by China was then continued and expanded upon by the Biden administration. Accordingly, it is likely to be a rare area of continuity in the years to come.

- **CFIUS**.
  - China: CFIUS will continue to closely scrutinize investments for national security risks from China (direct or indirect) and we assess CFIUS will continue to be a difficult environment for Chinese investment, particularly as it relates to critical technologies. Indeed, although in previous years Chinese investors successfully closed on deals in low risk businesses, the next administration may actively make the process more challenging for even low-risk deals as part of its broader initiatives to counter China economically.
  - Middle East: CFIUS may decrease its scrutiny of Middle Eastern sovereign wealth funds and similarly is likely to apply less scrutiny to private equity transactions.
  - Taiwan: Bolstered by statements President-elect Trump has made on Taiwan's role in the global semiconductor supply chain, CFIUS may become a more challenging process for Taiwanese investors, at least in relation to semiconductor deals and other critical technology businesses.
- **Outbound Investment Security Program**. The practical implications for the outbound program with the change in administration are difficult to predict because the rules will only become effective in the final weeks of the outgoing administration. That said, we assess the new administration will likely aggressively enforce the restrictions and may even seek to expand the scope of the technologies or countries of concern that are subject to the program.
- **Export Controls**. We expect the enforcement efforts of the DTSF and OICTS to continue to grow, particularly with respect to enforcement and investigation targeting China and Iran. Likewise, the incoming administration will likely continue to employ restrictive export controls on China with respect to many emerging technologies. One area to watch in particular will be how export controls on AI technologies are treated by the new administration, as maintaining U.S. leadership in the AI development race has been identified as a key priority.

* * *

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

Jessica S. Carey
+1-212-373-3566
jcarey@paulweiss.com

John P. Carlin
+1-202-223-7372
jcarlin@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Nicole Succar
+1-212-373-3624
nsuccar@paulweiss.com

Peter Carey
+1-202-223-7485
pcarey@paulweiss.com

Samuel Kleiner
+1-212-373-3797
skleiner@paulweiss.com

Nathan Mitchell
+1-202-223-7422
nmitchell@paulweiss.com

Associates Sean S. Malone, Benjamin M. Miller-Gootnick, and Joshua R. Thompson contributed to this Client Memorandum.

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

L. Rush Atkinson	Jessica S. Carey	John P. Carlin	Roberto J. Gonzalez
Melinda Haag	Jeh Charles Johnson	Brad S. Karp	Loretta E. Lynch
Mark F. Mendelsohn	Jeannie S. Rhee	Nicole Succar	