Debevoise & Plimpton

FCPA Update
October 2026
Volume 18
Number 3



# FCPA Update

A Global Anti-Corruption Newsletter



Also in this issue:

7 Treasury Proposes Significant Expansion of Outbound Investment Security Program

Click here for an index of all FCPA Update articles

If there are additional individuals within your organization who would like to receive *FCPA Update*, please email prohlik@debevoise.com, eogrosz@debevoise.com, or pferenz@debevoise.com

## UK Serious Fraud Office Introduces Whistleblower Payments and Revises Self-Reporting Guidance

In October 2026, the UK Government and the Serious Fraud Office ("SFO") issued two announcements that may have a significant impact on the SFO's future direction. First, the Government published a consultation proposing financial rewards for whistleblowers who provide the SFO with information leading to successful enforcement action.[1] A few days later, the SFO updated its corporate cooperation guidance to provide a mechanism for companies that are considering self-reporting to contact the SFO's General Counsel for discussions before committing to a formal self-report.

Continued on page 2

1. Department for Business, Innovation, Science and Trade, Attorney General's Office, Home Office, Serious Fraud Office, Kate Dearden MP, and The Rt Hon Jonathan Reynolds MP, "Open consultation – Whistleblowing" (Oct. 12, 2026), https://www.gov.uk/government/consultations/whistleblowing.

**UK Serious Fraud Office Introduces Whistleblower Payments and Revises Self-Reporting Guidance**

Continued from page 1

Both developments point in the same direction: through incentivizing those with information about potential white-collar crime to come forward, the SFO is aiming for a major boost to its pipeline of cases. Given its subdued activity in recent years with respect to major corporate crime matters – both in terms of new investigations announced and successfully resolved – the SFO will be hoping these steps can help it reverse that trend.

## New Whistleblower Incentivization Program

Historically, UK government agencies have not supported schemes to reward whistleblowers financially, in the belief that individuals who are aware of wrongdoing will generally want to "do the right thing" by reporting issues to their employer or (if necessary) to the authorities. That attitude has shifted significantly in the past five to 10 years, as it has become clear how vital whistleblowers can be in uncovering criminal activity and how harmful the consequences can be for them. It has also become apparent that UK authorities have been missing out on whistleblowing reports that have instead gone to U.S. authorities that do provide financial incentives: UK nationals are reportedly the second most frequent overseas users of the Securities and Exchange Commission whistleblower program.

The SFO's proposed whistleblower program implements a recommendation by Jonathan Fisher KC in his July 2026 Independent Review of Disclosure and Fraud Offences, and will very likely be modelled on similar programs run by its U.S. counterparts, the SEC and the Department of Justice:

- The SEC's long-standing whistleblower award program has paid out approximately $2 billion to 400 whistleblowers, with the highest award being $279 million in 2023. Following an enforcement action in which a penalty over $1 million is imposed, a whistleblower who provided high-quality, original information to the SEC may be awarded between 10 percent and 30 percent of the penalty amount.
- The DOJ Criminal Division launched a three-year "Corporate Whistleblower Awards Pilot Program" in August 2024, which has received over 1,800 tips. Some of these have led to criminal investigations, but so far none have resulted in awards. Whistleblowers may receive up to 30 percent of the first $100 million in net proceeds forfeited and up to five percent of any net proceeds forfeited between $100 million and $300 million.

Continued on page 3

**UK Serious Fraud Office Introduces Whistleblower Payments and Revises Self-Reporting Guidance**

Continued from page 2

The Government has outlined a few elements of its preferred approach to the SFO's whistleblower scheme:

- To qualify for an award, the information provided by the whistleblower must be significant and original and must lead to a successful enforcement outcome against company, such as a criminal conviction or a Deferred Prosecution Agreement ("DPA").
- Any reward will be calculated as a percentage of the fine or financial penalty imposed on the company and will only be paid once the case has concluded and all appeal rights have been exhausted. A percentage range will be set, with the exact amount determined according to a range of factors (such as the value of the information, the whistleblower's level of cooperation, and any complicity in the criminality); and
- Where multiple individuals provide different pieces of information, the reward can be shared among them.

"Both developments point in the same direction: through incentivizing those with information about potential white-collar crime to come forward, the SFO is aiming for a major boost to its pipeline of cases."

However, many details of the program are now open for public input through the consultation process, including:

- Who will be responsible for determining whether a whistleblower is eligible for a reward and calculating its value (the SFO, the courts, or another body);
- The criteria for a whistleblower to be eligible for a reward (for example, whistleblowers could be ineligible if they had a legal duty to report the information, were culpable in the offending, or obtained the information illegally);
- How the reward should be calculated (the percentage range, relevant factors, and any cap on the maximum value of payouts);
- Whether a criminal offence should be introduced for individuals who knowingly make false reports; and
- Whether a criminal offence should be created for harassing or intimidating whistleblowers who report to the SFO.

Continued on page 4

UK Serious Fraud Office Introduces Whistleblower Payments and Revises Self-Reporting Guidance

Continued from page 3

## Updated Corporate Cooperation Guidance

After a six-year gap between the two previous versions of its corporate cooperation guidance, the SFO has now revised the April 2025 guidance that has been in place for only 18 months.[2] The key changes are that:

- The SFO has introduced a mechanism for a company's legal advisors to contact the SFO General Counsel directly to discuss a potential self-report, with the company remaining anonymous at that stage. Its legal advisors will then be invited to a meeting with the SFO General Counsel;
- The SFO has made firm commitments to contact a company within 48 hours if it self-reports or has a query and to provide regular updates throughout the self-reporting process (these were previously expressed as aspirational goals);
- Wherever possible, the SFO will conclude DPA negotiations within six months of a company accepting an invitation to negotiate (rather than within six months of the SFO sending the company an invitation to negotiate); and
- As an additional example of exemplary cooperative conduct by a company ("genuine" cooperation with the SFO's investigation being required for a company to be invited to negotiate a DPA), the SFO states that the company should proactively consider key areas of risk across its business, including taking proportionate steps to ensure that the full extent of any potential criminality has been reported to the SFO.

## Analysis

If the SFO's whistleblower program is designed well – with broad eligibility criteria and enabling significant financial rewards – it could be the "gamechanger" that the SFO has been seeking to revive what is generally perceived to be a somewhat depressed investigation and enforcement pipeline in the area of cross-border and large-scale corporate crime. In many investigations, the wrongdoing was known only by a relatively small number of participants and was carefully concealed from anyone outside that circle. Information from a whistleblower, whether that is someone who was directly involved in the wrongdoing or has some second-hand knowledge that has raised his or her suspicions, is often crucial in identifying issues and breaking open a scheme. Without some inside knowledge, wrongdoing can go undetected for years or may never be unearthed.

Continued on page 5

2. Serious Fraud Office, "Make a corporate self-report" (Oct. 13, 2026), https://www.gov.uk/government/publications/make-a-corporate-self-report. *See also* Karolos Seeger, et al., "New Corporate Cooperation Guidance from the UK SFO: More Carrot and Less Stick – the British Version" FCPA Update, Vol. 16, No. 10 (May 2025), https://www.debevoise.com/insights/publications/2025/05/fcpa-update-may-2025.

**UK Serious Fraud Office Introduces Whistleblower Payments and Revises Self-Reporting Guidance**

Continued from page 4

The new program will also require considerable resourcing from the SFO to triage tips, liaise with whistleblowers, and handle an increased investigation caseload. Even then, there is no guarantee that the result will be more corporate convictions and DPAs, especially in the short to medium term, as can be seen from the DOJ Criminal Division's whistleblower program. Importantly, however, companies will need to bear in mind the higher likelihood of employees and third parties reporting misconduct directly to the SFO in the hope of a reward. This means that issues with potential criminal implications should be rapidly investigated and may weigh in favor of the company self-reporting to the SFO at an early stage.

The SFO's new mechanism for discussions between its General Counsel and a company's legal advisors when considering self-reporting appears beset with greater uncertainty. The only indication the SFO has given of the potential content of such discussions is the question whether the SFO is the correct agency to receive a self-report. That does not immediately appear as an obvious question companies have hitherto struggled to grapple with by themselves (i.e., without the SFO's General Counsel's input). Apart from providing information about self-reporting and its potential benefits, which, again, a well-advised company will already understand, it is questionable whether the SFO General Counsel would be willing to go further in such discussions – for example, by providing hypothetical views on the gravity of the conduct involved in the matter (so as to assist the company with the self-reporting question), committing to an investigation timeline or process in the event of a self-report, or commenting specifically on the nature and extent of its likely coordination and cooperation with specific overseas authorities in the case of a cross-border matter. What seems almost certain is that the SFO will not want to return to the level of engagement with companies that was possible under the tenure of its former Director pre-2012 and much criticized by subsequent Directors thereafter, on the basis that it amounted to providing advice to companies which was inappropriate for an investigative and prosecutorial body such as the SFO, or offering inappropriate incentives (in the form of promises of a civil as opposed to criminal outcome) in the event of a self-report.

Notwithstanding these reservations about the new mechanism, the signal to companies that the SFO is now willing to have a dialogue with ethical corporates that are considering self-reporting, and to do so outside the strictures of the formal

Continued on page 6

**UK Serious Fraud Office Introduces Whistleblower Payments and Revises Self-Reporting Guidance**

Continued from page 5

self-reporting process itself, should be welcomed as a very positive step that can only enhance the SFO's standing as an effective and reasonable corporate criminal investigative and enforcement agency.

**Karolos Seeger**

**Andrew H. W. Lee**

*Karolos Seeger is a partner in the London office. Andrew H. W. Lee is a counsel in the London office. Full contact details for each author are available at www.debevoise.com.*

Continued on page 7

# Treasury Proposes Significant Expansion of Outbound Investment Security Program

On October 22, 2026, the U.S. Treasury Department's Office of Investment Security ("Treasury") issued its long-awaited notice of proposed rulemaking (the "NPRM") to implement provisions of the Comprehensive Outbound Investment National Security Act of 2025 (the "COINS Act").[1] The COINS Act was enacted on December 18, 2025, and directs Treasury to update and amend its existing Outbound Investment Security Program ("OISP") regulating certain outbound investments by U.S. persons.

The OISP regulations at 31 CFR Part 850 (the "Part 850 Regulations") currently prohibit or require notice to Treasury of certain investments ("covered transactions") by U.S. persons or their controlled foreign entities involving targets or counterparties with specified connections to the People's Republic of China (together with the Special Administrative Regions of Hong Kong and Macau, "China") engaged in certain activities in the semiconductors and microelectronics, artificial intelligence ("AI") or quantum information technologies sectors.

As directed or authorized by the COINS Act, the NPRM proposes several changes to the current OISP, including expanding restrictions to cover investments involving additional countries and technologies, broadening the categories of transactions prohibited for U.S. persons and adding certain new processes. Notably, the proposed regulations under the NPRM (the "Proposed Rule") would broadly prohibit U.S. persons from investments in targeted entities that develop any AI system and prohibit various biotechnology investments.

The Proposed Rule would reformulate terminology and target "covered national security transactions" involving "covered foreign persons" that are engaged in a "notifiable technology" or "prohibited technology." We review each of these concepts, proposed exceptions from OISP requirements and proposed new procedural mechanisms below. In Appendix A, we provide a chart summarizing the sectors and technologies covered under the Proposed Rule and highlight differences from the existing OISP.

Treasury has requested comments on the NPRM by December 7, 2026.

Continued on page 8

1. Outbound Investment Security Program Regulations, 91 Fed. Reg. 67396 (proposed Oct. 26, 2026), *available* here. *See also* Debevoise Update, *Treasury's First Outbound Investment Penalty: Implications for Private Fund Sponsors and Cross-Border Investment Activity* (Oct. 14, 2026), *available* here; Debevoise Update, *The Outbound Investment Rule: Guidance on Publicly Traded Securities* (Jan. 7, 2026), *available* here; Debevoise In Depth, *New U.S. Law Expands Outbound Investment Regime and Sanctions Authorities* (Dec. 17, 2025), *available* here; Debevoise In Depth, *Treasury Finalizes U.S. Outbound Investment Restrictions* (Nov. 8, 2024), *available* here.

Treasury Proposes Significant Expansion of Outbound Investment Security Program
Continued from page 7

## Interaction with Part 850 Regulations

The current OISP was implemented by Treasury pursuant to Executive Order 14105 and authorized under the International Emergency Economic Powers Act. The Part 850 Regulations establishing the current OISP went into effect on January 2, 2025.

The NPRM would establish a separate, though broadly similar, regulatory framework under the COINS Act by adding a new 31 CFR Part 851.[2] The Proposed Rule would not remove the existing Part 850 Regulations, which would remain in effect and continue to apply to transactions and other activities occurring on or after January 2, 2025, and before the effective date of the final regulations implementing the COINS Act.

## Who Would Be Obligated to Comply with the Proposed Rule?

The Proposed Rule retains the current approach and existing definitions under the Part 850 Regulations for "U.S. person." Accordingly, the Proposed Rule would apply to any U.S. citizen, lawful permanent resident, entity organized under U.S. law (including any foreign branch of such entity) and person in the United States.

The Proposed Rule also continues the current application to "controlled foreign entities" of U.S. persons. Under the Part 850 Regulations and the Proposed Rule, a "controlled foreign entity" is a non-U.S. entity of which a U.S. person is a "parent," which includes a non-U.S. entity as to which the U.S. person (i) holds, directly or indirectly, more than 50% of the entity's outstanding voting interests or voting power of its board, (ii) is the general partner, managing member or equivalent (iii) or is the investment adviser to an entity that is a pooled investment fund. A U.S. person would continue to be required (i) to take "all reasonable steps" to prevent and prohibit any transaction by its controlled foreign entity that would be a prohibited transaction if engaged in by a U.S. person and (ii) to file a notice with Treasury for any transaction undertaken by its controlled foreign entity that the controlled foreign entity or the U.S. person knew at the time of the transaction would be a notifiable transaction if engaged in by a U.S. person.

In the NPRM, Treasury indicates it is considering whether to expand the definition of a "parent" to encompass certain sub-advisers to a non-U.S. fund and the general manager (or equivalent) of a non-U.S. entity. Such change potentially could expand the scope of controlled foreign entities covered under the Proposed Rule.

Continued on page 9

2. The NPRM does not address the extent to which Treasury's existing OISP frequently asked question guidance would be applicable to new 31 CFR Part 851 but suggests that at least some existing guidance may be re-issued to apply to the new regulations.

Treasury Proposes Significant Expansion of Outbound Investment Security Program
Continued from page 8

## What Investment Activities Are Targeted Under the Proposed Rule?

The Proposed Rule expands the list of "countries of concern" targeted under the OISP. It also revises the current OISP definition of a "covered foreign person" to focus on a foreign person's connections to a country of concern without regard to the activities in which that person engages.

### Countries of Concern

As directed by the COINS Act, the Proposed Rule expands the definition of "country of concern" beyond China to also include (i) Cuba, (ii) Iran, (iii) North Korea, (iv) Russia and (v) Venezuela under the regime of Nicolás Maduro Moros.

- Treasury clarified in the NPRM and related guidance that the Venezuelan regime of Nicolás Maduro Moros no longer exists and that the Venezuelan government under Delcy Rodríguez is not the regime of Nicolás Maduro Moros. Accordingly, Venezuela is not a country of concern under the Proposed Rule.

"[T]he [notice of proposed rulemaking] proposes several changes to the current [Outbound Investment Security Program], including expanding restrictions to cover investments involving additional countries and technologies, broadening the categories of transactions prohibited for U.S. persons and adding certain new processes."

### Covered Foreign Person

The Proposed Rule defines a "covered foreign person" as:

1. An individual who is a citizen or permanent resident of a country of concern (other than U.S. citizens or permanent residents);
2. An entity incorporated in, organized under the laws of or having a principal place of business in a country of concern;
3. An individual who is a member of the Central Committee of the Chinese Communist Party or is otherwise a member of the political leadership of a country of concern;
4. The government of a country of concern or any person acting for or on behalf of such government;
5. An entity that is, directly or indirectly, 50% or more owned in the aggregate by or subject to the direction or control of the foregoing persons;

Continued on page 10

**Treasury Proposes Significant Expansion of Outbound Investment Security Program**

Continued from page 9

6. An entity in which one or more covered foreign persons meeting the criteria of the foregoing factor five in the aggregate hold 50% or more of the voting interests, voting power of the board or equity interests; or

7. An entity directly or indirectly holding a board seat on, a voting or equity interest in or any contractual power to direct or cause the direction of the management or policies of one or more covered foreign persons that engage in a covered notifiable or prohibited technology and from or through which the entity derives more than 50% of specified financial metrics from such covered foreign persons in the aggregate, subject to limited exceptions.

Although the Proposed Rule's definition of "covered foreign person" largely incorporates the current Part 850 Regulations' definition of a "person of a country of concern," there is a notable change. The relevant concept in the current Part 850 Regulations captures entities over which the Chinese government has the "power to direct or cause the direction of management and policies." However, under the fifth factor above, the Proposed Rule's covered foreign person definition expands this concept to capture any entity "directly or indirectly subject to the direction or control of" any person described in factors one through four.

The Proposed Rule further offers new interpretative guidance that explains "subject to the direction or control" means that a person described in factor one through four "has the power, directly or indirectly, to direct or cause the direction of the management or policies of such entity (whether through the ownership of voting securities, by contract, or otherwise)." Notably, the Proposed Rule is formulated and will be enforced by the same office that provides administrative support for the Committee on Foreign Investment in the United States ("CFIUS"), which, in that context, can find minority shareholders holding ownership interests as low as 10% to have similar control powers.

## What Transactions Are Covered Under the Proposed Rule?

The Proposed Rule uses a new term from the COINS Act—"covered national security transaction"—in place of the Part 850 Regulations' use of "covered transactions," but the new term, as a practical matter, covers essentially the same conduct. A "covered national security transaction" under the Proposed Rules involves the following transactions, described generally:

1. Acquisition of an equity or contingent equity interest (including through foreclosure on collateral where the debtholder takes possession of pledged equity);

2. Provision of a loan or similar debt financing arrangement that provides certain equity-like financial or governance rights;

Continued on page 11

**Treasury Proposes Significant Expansion of Outbound Investment Security Program**
Continued from page 10

3. Entrance into a joint venture;
4. Conversion of a contingent equity interest or debt to an equity interest;
5. A greenfield investment or other corporate expansion;
6. Direction of a transaction by a foreign person that the U.S. person knows at the time of the transaction would constitute a transaction described in categories 1–5 above if engaged in by a U.S. person; or
7. Certain limited partner ("LP") or equivalent investments in non-U.S. pooled investment funds.

The sixth transaction type incorporates the concept of "knowingly directing" present in the Part 850 Regulations into the Proposed Rule "covered national security transaction" framework. Under the Proposed Rule, to engage in such a covered transaction, the relevant U.S. person must still have "authority, individually or as part of a group, to make or substantially participate in decisions on behalf of a foreign person (including being an officer or director of, or otherwise possessing executive responsibilities with respect to, the foreign person) and, individually or as part of a group, exercise[] that authority to, direct, order, decide upon, or approve a transaction that the U.S. person knows would be a covered national security transaction if engaged in by a U.S. person," and the Proposed Rule continues to suggest recusal for a U.S. person to avoid being treated as directing a covered national security transaction by a non-U.S. person.

Whereas the Part 850 Regulations restrict U.S. persons from knowingly directing a transaction by a non-U.S. person that would be a prohibited transaction if undertaken by a U.S. person, the Proposed Rule would also encompass notifiable transactions, triggering a notice obligation for a U.S. person knowingly directing a transaction by a foreign person that would be notifiable if engaged in by a U.S. person.

## What Technologies Are Targeted Under the Proposed Rule?

The Proposed Rule applies to the three technology sectors currently covered by the Part 850 Regulations (*i.e.*, semiconductors and microelectronics, AI systems and quantum information technologies), separates a new category (high-performance computing and supercomputing) from the semiconductors category and adds two sectors (hypersonic systems and biotechnology).

High-performance computing and hypersonic systems are expressly listed in the COINS Act, and Treasury was obligated to include these in the Proposed Rule.

Continued on page 12

**Treasury Proposes Significant Expansion of Outbound Investment Security Program**
Continued from page 11

Further, Treasury, as authorized under the COINS Act, has determined the biotechnology sector enables the military, intelligence, surveillance or cyber-enabled capabilities of countries of concern and, accordingly, proposes to add certain technologies and products within that sector as prohibited technologies (there are no notifiable activities related to biotechnology).

As described below, the Proposed Rule would meaningfully expand every category of covered technologies, including, most notably, prohibiting covered national security transactions involving covered foreign persons engaged in the development of any AI system (referred to as "super intelligence" ("SI") systems in the Proposed Rule), without regard to the system's technical capabilities or thresholds. Please see Appendix A for a summary of the sectors and technologies covered under the Proposed Rule.

The Proposed Rule also expands the existing definition of the term "develop" used to describe certain activities in the prohibited and notifiable technology definitions. The expanded definition includes engaging in covered activities through or in collaboration with affiliates and providing high-level oversight, direction, approval, conceptual input or strategic planning in connection with the specified activities. These changes broaden the range of activities engaged in by a covered foreign person that are treated as a prohibited or notifiable technology under the Proposed Rule.

### AI (SI) Systems

As noted above, the Proposed Rule defines "prohibited technology" to cover the development of any SI system, in contrast to the distinction under the Part 850 Regulations between prohibited and notifiable AI covered activities based on the compute required to train the model or the designed or intended end use of the AI system. In the NPRM, Treasury explains that rapid advances by countries of concern in the development, adoption and use of SI capabilities since the Part 850 Regulations were published warrant a broader prohibition. Treasury also notes that its "just-say-no" approach would eliminate the need for U.S. persons to ascertain the technical capabilities or thresholds of SI systems developed by covered foreign persons.

- The Proposed Rule's definition of an "SI system" generally retains the Part 850 Regulations' definition but expands the current rules by expressly encompassing machine-based systems capable of generating content and embodied SI systems, such as robotic or other autonomous or unmanned systems that operate using an SI system.

Continued on page 13

**Treasury Proposes Significant Expansion of Outbound Investment Security Program**

Continued from page 12

- Although the Proposed Rule continues to distinguish between a person developing an SI system and merely using an off-the-shelf third-party SI system strictly for internal, non-commercial purposes, because an SI system is defined to encompass any "data system, software, hardware, application, tool, or utility that operates in whole or in part using an SI system," it appears that developing any software, applications, utilities, etc. that call on any SI system for any purpose may be a prohibited technology.

### High-Performance Computing and Supercomputing

Although newly identified as a separate technology sector under the COINS Act, high-performance computing and supercomputing technologies were already addressed under the Part 850 Regulations. The Proposed Rule expands the prohibited technology definition to include high-bandwidth memory with a specified memory bandwidth density and additional categories of advanced integrated circuits and expands the notifiable technology definition to include high-bandwidth, low-latency interconnects used in high-performance computing.

"[T]he Proposed Rule would meaningfully expand every category of covered technologies, including, most notably, prohibiting covered national security transactions involving covered foreign persons engaged in the development of any AI system … without regard to the system's technical capabilities or thresholds."

### Hypersonic Systems

The Proposed Rule defines a "hypersonic system" as "a vehicle or weapon delivery system capable of sustained atmospheric or very low Earth orbit flight at speeds of Mach 5 or greater, including hypersonic glide vehicles, hypersonic cruise missiles, hypersonic air-launched or aero-ballistic missiles, maneuvering reentry vehicles, and reusable hypersonic vehicles."

Under the Proposed Rule, prohibitions apply to both military and civilian hypersonic systems; propulsion systems capable of enabling hypersonic flight; certain related and enabling technologies associated with hypersonic systems; certain materials designed to withstand atmospheric conditions at hypersonic speeds; and facilities capable of testing a hypersonic system. The Proposed Rule requires notice for transactions involving sensors, control equipment and software for hypersonic systems and other dual-use materials that can be used in hypersonic systems.

Continued on page 14

Treasury Proposes Significant Expansion of Outbound Investment Security Program
Continued from page 13

### Biotechnology

The Proposed Rule prohibits a broad range of biotechnology activities and equipment. Prohibited technology includes certain bio-derived compounds or materials, including pharmaceutical compounds among others; brain computer interfaces; biomanufacturing equipment and facilities; biotechnology or equipment involved in biological design, sequencing and other activities; bioinformatics tools; and hardware or software for automated scientific discovery or experimentation. The Proposed Rule does not establish a separate category of notifiable biotechnology activities.

Treasury acknowledges that the breadth of its proposed biotechnology restrictions could have significant implications for public health or U.S. businesses in the biotechnology sector and specifically invites comment on its proposed approach.

### Transactions Involving Listed Persons

The Proposed Rule expands the circumstances in which an otherwise notifiable technology is treated as a prohibited technology based on a covered foreign person's or relevant joint venture's connections to parties on certain U.S. government lists.

Under the Proposed Rule, as under the Part 850 Regulations, an otherwise notifiable technology engaged in by a covered foreign person or relevant joint venture constitutes a prohibited technology if that covered foreign person or joint venture appears on one of several specified U.S. government lists. In addition to the lists referenced in the existing OISP for this purpose, the Proposed Rule would add (i) the list of Chinese military companies maintained under Section 1260H of the National Defense Authorization Act for Fiscal Year 2021 and (ii) the Office of Management and Budget's list of biotechnology companies of concern under the BIOSECURE Act.

Additionally, unlike the Part 850 Regulations, the Proposed Rule would treat as prohibited any otherwise notifiable activity of a covered foreign person or joint venture if any subsidiary or affiliate of such entity is included on one of the specified U.S. government lists. Treasury indicates this approach is intended to deter a listed person from establishing a subsidiary to engage in a notifiable technology and participate in a covered national security transaction that the listed person could not itself participate in. The broad definition of "affiliate" to include entities under common control would further expand the scope of activity treated as prohibited.

Continued on page 15

Continued from page 14

## What Exceptions Are Available Under the Proposed Rule?

The Proposed Rule generally retains most, but not all, exceptions provided under the Part 850 Regulations, with certain modifications to some exceptions.

Several new exceptions, including some particularly applicable to financial services activities, are proposed to be added. These include the following:

- **Secondary transactions**. The Proposed Rule expressly excepts "a transaction secondary to a covered national security transaction," including:
  - contractual arrangements (not including contractual arrangements for technology transfer or technical knowledge transfer) or the procurement of material inputs for any covered national security transaction (such as raw materials);
  - bank lending;
  - processing, clearing or sending of payments by a bank;
  - underwriting services including, but not limited to, the temporary acquisition of an equity interest for the sole purpose of facilitating underwriting services;
  - debt rating services;
  - prime brokerage;
  - global custody;
  - equity research or analysis; or
  - other similar services.
- **Ancillary transactions**. The Proposed Rule separately excepts certain ancillary transactions undertaken by financial institutions, including:
  - processing, clearing or sending payments and cash transactions for or to a covered foreign person;
  - underwriting services, including the temporary acquisition of an equity interest in a covered foreign person for the sole purpose of facilitating underwriting services;
  - credit rating services on behalf of a covered foreign person; or
  - other services ordinarily incident to and part of the provision of financial services on behalf of a covered foreign person, such as opening deposit accounts, direct custody services, foreign exchange services, remittances services and safe deposit services.

Continued on page 16

Treasury Proposes Significant Expansion of Outbound Investment Security Program
Continued from page 15

- **De minimis transactions**. The Proposed Rule introduces an exception for notifiable transactions (but not prohibited transactions) where neither the value of the covered national security transaction, nor the provision of funds or other consideration to the relevant covered foreign person or joint venture, in the aggregate across the preceding 12 months exceeds $50,000.
- **Grandfathered transactions**. Any transaction completed before December 18, 2025 (the date of enactment of the COINS Act), although a transaction prior to this date may be subject to the Part 850 Regulations.

With respect to the secondary transactions exception, Treasury invites comment on, among other things, whether the exception for "bank lending" would except all "banks" from covered national security transactions involving provision of a loan or similar debt financing.

The COINS Act also contemplates an exception for "ordinary or administrative business transactions." The Proposed Rule includes this exception, but Treasury opted not to propose a definition for the exception, indicating that it believes such transactions generally would already be covered under the exceptions for secondary and ancillary transactions or would not be a covered national security transaction in the first place.

"The Proposed Rule establishes a new process through which a person with a direct financial interest in an actual, non-hypothetical prospective transaction may request non-binding feedback from Treasury regarding whether the transaction would constitute a prohibited transaction."

The Proposed Rule would not carry forward the existing exception under the Part 850 Regulations for investments in securities issued by business development companies, which exception was not provided for under the COINS Act. The Proposed Rule also would not include an exception for securities issued by non-U.S. investment companies subject to foreign regulatory oversight comparable to that of the U.S. Securities and Exchange Commission. Treasury indicates it welcomes comment on these potential other exceptions.

Continued on page 17

Continued from page 16

## What Additional OISP Mechanisms Would Be Implemented Under the Proposed Rule?

The Proposed Rule implements some, but not all, of the additional administrative OISP mechanisms contemplated under the COINS Act. It also requires additional information to be included in required notices submitted to Treasury.

### Non-Binding Feedback

The Proposed Rule establishes a new process through which a person with a direct financial interest in an actual, non-hypothetical prospective transaction may request non-binding feedback from Treasury regarding whether the transaction would constitute a prohibited transaction. Requests would need to be submitted in writing and the material terms of the prospective transaction would need to be identified in a binding written agreement or other binding document to establish that the transaction is not hypothetical.

A requester can request either confidential written feedback or anonymized public guidance, and Treasury has discretion to provide confidential feedback, issue anonymized public guidance or decline to respond. Any feedback would be non-binding and would not constitute a formal authorization, license, exemption or waiver, although Treasury may consider, among other factors, whether a person sought and reasonably acted consistent with non-binding feedback in determining an appropriate response to an OISP violation.

### Submission of Confidential Information Regarding Covered Foreign Persons

The Proposed Rule also establishes a process through which any person can confidentially submit information to Treasury regarding whether a foreign person is a covered foreign person engaged in a prohibited or notifiable technology. The Proposed Rule sets out the information required to be submitted for these purposes.

### Public Database of Covered Foreign Persons

Although the COINS Act authorizes Treasury to establish a publicly accessible, non-exhaustive database identifying covered foreign persons engaged in prohibited or notifiable technologies, the Proposed Rule does not establish such a database. Treasury states in the NPRM that it is actively considering whether and how to establish such a database and welcomes comment on this matter.

Continued on page 18

Treasury Proposes Significant Expansion of Outbound Investment Security Program
Continued from page 17

### Notice Information Requirements

The Proposed Rule expands the information that must be included in the notice required to be submitted to Treasury for a notifiable transaction. The additional required items include information that Treasury indicates it typically has sought through follow-up requests under the existing OISP and include, among other things, information about the relevant U.S. person and covered foreign person, the relevant transaction and transaction documentation.

**Satish M. Kini**

**Aseel M. Rabie**

**Robert T. Dura**

**Jonathan R. Wong**

*Satish M. Kini and Aseel Rabie are partners in the Washington, D.C. office. Robert T. Dura is a counsel in the Washington, D.C. office. Jonathan R. Wong is an associate in the London office. Full contact details for each author are available at www.debevoise.com.*

Continued on page 19

## Appendix A—Covered Sectors and Technologies under Proposed Rule[3]

| Sector | Prohibited Technology | Notifiable Technology |
|---|---|---|
| Semiconductors and microelectronics | Electronic design automation software for integrated circuits ("ICs") or advanced packaging<br><br>Specified fabrication or advanced packaging equipment or technology<br><br>Packaging of ICs using advanced packaging techniques<br><br>Specified advanced ICs, including **radiation-hardened and photonic ICs, additional advanced ICs and high-bandwidth memory** | ICs not otherwise prohibited<br><br>**Equipment for IC design, fabrication or packaging not otherwise prohibited** |
| Super intelligence systems | **Development of any SI system (expanded prohibition)** | None |
| Quantum information technologies | Quantum computers and critical components<br><br>Quantum sensing platforms for military, intelligence or surveillance uses<br><br>Quantum networks or quantum communications systems<br><br>**Software, algorithms and applications for quantum computing** | None |
| **High-performance computing and supercomputing** | Supercomputers above specified performance thresholds | **High-bandwidth, low-latency interconnects for high-performance computing** |

Continued on page 20

3. New technologies or sectors covered under the Proposed Rule are noted in bold.

| Sector | Prohibited Technology | Notifiable Technology |
|---|---|---|
| **Hypersonic systems** | **Hypersonic systems**<br><br>**Propulsion systems capable of enabling hypersonic flight**<br><br>**Certain materials designed for or intended to be used for a hypersonic system**<br><br>**Specialized infrastructure or facility for testing a hypersonic system**<br><br>**Certain enabling technologies associated with hypersonic systems** | **Sensors, control equipment and, as not otherwise prohibited, software for hypersonic systems**<br><br>**Certain dual-use materials capable of use in hypersonic systems** |
| **Biotechnology** | **Certain bio-derived restricted agents and toxins, energetic materials, novel or high-performance functional materials, biofuels, or pharmaceutical compounds**<br><br>**Brain-computer interfaces**<br><br>**Biomanufacturing equipment and related components, software or technology**<br><br>**Biological design and sequencing technologies**<br><br>**Bioinformatics tools**<br><br>**Hardware or software for automated scientific discovery or experimentation** | None |

# FCPA Update

FCPA Update is a publication of
Debevoise & Plimpton LLP

66 Hudson Boulevard
New York, New York 10001
+1 212 909 6000
www.debevoise.com

Washington, D.C.
+1 202 383 8000

San Francisco
+1 415 738 5700

London
+44 20 7786 9000

Paris
+33 1 40 73 12 12

Frankfurt
+49 69 2097 5000

Hong Kong
+852 2160 9800

Shanghai
+86 21 5047 1800

Luxembourg
+352 27 33 54 00

Andrew J. Ceresney
Co-Editor-in-Chief
+1 212 909 6947
aceresney@debevoise.com

David A. O'Neil
Co-Editor-in-Chief
+1 202 383 8040
daoneil@debevoise.com

Karolos Seeger
Co-Editor-in-Chief
+44 20 7786 9042
kseeger@debevoise.com

Douglas S. Zolkind
Co-Editor-in-Chief
+1 212 909 6804
dzolkind@debevoise.com

Philip Rohlik
Co-Executive Editor
+852 2160 9856
prohlik@debevoise.com

Andrew M. Levine
Co-Editor-in-Chief
+1 212 909 6069
amlevine@debevoise.com

Winston M. Paes
Co-Editor-in-Chief
+1 212 909 6896
wmpaes@debevoise.com

Jane Shvets
Co-Editor-in-Chief
+44 20 7786 9163
jshvets@debevoise.com

Erich O. Grosz
Co-Executive Editor
+1 212 909 6808
eogrosz@debevoise.com

Please address inquiries regarding topics covered in this publication to the editors.

All content © 2026 Debevoise & Plimpton LLP. All rights reserved. The articles appearing in this publication provide summary information only and are not intended as legal advice. Readers should seek specific legal advice before taking any action with respect to the matters discussed herein. Any discussion of U.S. Federal tax law contained in these articles was not intended or written to be used, and it cannot be used by any taxpayer, for the purpose of avoiding penalties that may be imposed on the taxpayer under U.S. Federal tax law.

Please note:
The URLs in *FCPA Update* are provided with hyperlinks so as to enable readers to gain easy access to cited materials.