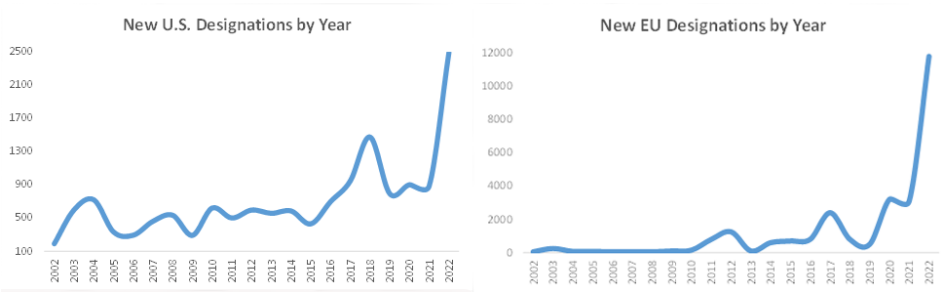
GIBSON DUNN

2022 Year-End Sanctions and Export Controls Update

Client Alert | February 7, 2023

Policymakers in Washington, London, and other allied capitals during 2022 pushed the outer limits of economic statecraft to tackle challenges ranging from Russia's full-scale invasion of Ukraine to China's growing military and technological capabilities. Notably, President Joe Biden continued his predecessor's approach of weaponizing different tools and executive offices in the economic coercion space—further blurring once clear distinctions between sanctions, export controls, import restrictions, tariffs, and foreign investment reviews. Breaking down longtime silos between those different policy instruments proved effective at exerting economic pressure on Moscow, Beijing, and other targets over the past year, and these tools will be a durable feature of U.S. and allied policy going forward. In addition to the breadth of economic tools employed by the United States, one of the year's most consequential developments was the Biden administration's emphasis on employing trade restrictions in close coordination with traditional allies and partners. In a sharp break from the prior administration, President Biden, on the campaign trail and through last year's comprehensive review of U.S. sanctions, articulated a strong preference for multilateral solutions to global challenges. That policy approach was put vividly into practice in 2022 following the Kremlin's further invasion of Ukraine as a coalition of more than 30 democracies—together accounting for more than half of global economic output—clamped severe restrictions on trade with Russia. Such close coordination magnified the impact of sanctions by making them more challenging to evade, and raised questions regarding whether coalition policymakers can muster a similarly united front in response to other pressing challenges like an increasingly powerful China. Despite their close alignment, small divergences between the United States, the European Union, and the United Kingdom—with respect to both targets and, more importantly, matters of interpretation such as whether entities controlled by a sanctioned party are restricted—presented daunting compliance challenges for multinational businesses. Over the past year, policymakers broke new ground by, for the first time ever, imposing sweeping trade controls on a major, globally connected economy—including adding a record-shattering number of (mostly Russian) individuals and entities to sanctions lists:



The past year was also remarkable for its many instances of genuine policy innovation, as officials immobilized Russia's foreign reserves, introduced a novel price cap on seaborne Russian crude oil and petroleum products, imposed unprecedented controls on China's access to advanced semiconductors, and laid the groundwork for possible new regimes in the United States and Europe to review outbound foreign investments. However, U.S. and allied governments were not the only active players. From Moscow to Beijing, targets of economic coercion have not sat still, imposing their own countermeasures, promulgating

Related People

Scott R. Toussaint

Irene Polieri

Chris R. Mullen

Judith Alison Lee

Adam M. Smith

Stephenie Gosnell Handler

Michelle M. Kirschner

Patrick Doris

Benno Schwarz

Katharina E. Humphrey

Attila Borsos

Christopher T. Timura

David A. Wolber

Allison Lewis

Nikita Malevanny

Sarah L. Pongrace

Anna Searcey

Samantha Sewall

Audi K. Syarief

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

regulations to impede domestic compliance with “unfriendly country” actions, and hindering the ability of outside parties to even learn about the ownership or control of certain parties that may be impacted by restrictions. In addition to governmental action, 2022 was notable for the extreme de-risking seen especially in Russia, with more than a thousand companies deciding to pull back from operations in that country before any regulation demanded it of them. This “self-sanctioning” was not part of the coalition’s strategy, and its implications for a diminished ability of allied policymakers to effectively calibrate measures going forward—when businesses will undoubtedly remain skittish—makes the entire canon of economic statecraft uncertain. Multinational enterprises must also contend with the U.S. Department of Justice’s emerging view of sanctions as the “new” Foreign Corrupt Practices Act—portending an uptick in civil and criminal enforcement activity. By any measure, 2022 was a historically busy period for the imposition of new trade controls, and the pace of policy change shows few signs of slowing during the year ahead. **Contents** I. Global Trade Controls on Russia A. Comprehensive Sanctions on Covered Regions of Ukraine B. Sectoral Sanctions C. Blocking Sanctions D. Export Controls E. Import Prohibitions F. New Investment Prohibitions G. Services Prohibitions H. Price Cap on Crude Oil and Petroleum Products I. Possible Further Trade Controls on Russia II. U.S. Trade Controls on China A. Uyghur Forced Labor Prevention Act B. Technological Competitiveness Legislation C. Export Controls D. Defense Department List of Chinese Military Companies E. Investment Screening III. U.S. Sanctions A. Iran B. Syria C. Venezuela D. Nicaragua E. Afghanistan F. Myanmar G. Crypto/Virtual Currencies H. Other Sanctions Developments IV. U.S. Export Controls A. Commerce Department B. State Department V. Committee on Foreign Investment in the United States (CFIUS) A. CFIUS Annual Report B. National Security Factors C. Enforcement and Penalty Guidelines D. Outbound Investment Screening VI. European Union A. Trade Controls on China B. Sanctions Developments C. Export Controls Developments D. Foreign Direct Investment Developments VII. United Kingdom A. Trade Controls on China B. Sanctions Developments C. Export Controls Developments D. Foreign Direct Investment Developments **I. Global Trade Controls on Russia**

Following the Kremlin’s further invasion of Ukraine in February 2022, leading industrial economies—including the United States, the European Union, the United Kingdom, Canada, Australia, and Japan—swiftly imposed aggressive and coordinated trade controls on Russia. Spurred by global outrage and fierce Ukrainian resistance, 2022 saw the imposition of a cascade of restrictions that would have been unthinkable in even the recent past, including comprehensive sanctions on Russian-occupied regions of Ukraine, wide-ranging sectoral sanctions, blocking sanctions, export controls, import bans, new investment bans, services bans, and an innovative price cap on seaborne Russian crude oil and petroleum products. Taken together, these measures—which target key pillars of Russia’s economy (and its principal sources of hard currency) such as the country’s financial sector, energy sector, and military-industrial complex—were calculated to deny the Kremlin the resources needed to prosecute the war in Ukraine and degrade Russia’s ability to project power abroad. As the war in Ukraine nears its first anniversary, allied trade restrictions appear to be exacting a toll on Russia’s economy, which, despite soaring energy prices, contracted during 2022. Notably, more than a thousand companies have ceased or curtailed their operations in Russia since the start of the war—an exodus that by and large was not mandated by regulation but that nonetheless threatens to further dim Russia’s long-term growth prospects. Meanwhile, the coalition continues to hold additional policy options in reserve. Depending upon how events unfold, the allies could potentially further restrict dealings involving Russia by imposing blocking sanctions on additional Russian elites, designating the Government of the Russian Federation, moving to seize Russian assets to fund Ukraine’s reconstruction, or expanding existing sanctions and export controls to include a complete embargo on trade in goods and services. **A. Comprehensive Sanctions on Covered Regions of Ukraine** On February 21 and 22, 2022, the United States and key allies imposed comprehensive sanctions on the Russia-backed separatist regions of Ukraine known as the Donetsk People’s Republic (“DNR”) and the Luhansk People’s Republic (“LNR”). This initial round of sanctions came as President Putin recognized the two breakaway regions as independent states and quickly ordered Russian troops to enter the regions for an ostensible “peacekeeping” mission. Just hours after the dramatic Russian announcement, President Biden signed Executive

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

Order ("E.O.") 14065, which imposes broad, jurisdiction-wide sanctions on the DNR and LNR, plus any other regions of Ukraine as may be determined by the U.S. Secretary of the Treasury (collectively, the "Covered Regions"). As we wrote in an earlier client alert, that measure by President Biden is nearly identical to Executive Order 13685, which announced President Barack Obama's imposition of comprehensive sanctions on the Crimea region of Ukraine in 2014. In particular, E.O. 14065 prohibits: (1) new investment in the Covered Regions by a U.S. person; (2) the importation into the United States of any goods, services, or technology from these regions; as well as (3) the exportation from the United States, or by a U.S. person, of any goods, services, or technology to these regions. The Order further authorizes blocking sanctions on any person determined by the Secretary of the Treasury to be a person operating in the Covered Regions. The European Union and the United Kingdom have adopted similarly broad restrictions, yet these are not total bans on dealings with the regions. EU restrictions target Donetsk, Luhansk, Kherson, and Zaporizhzhia, while UK restrictions only target Donetsk and Luhansk. As a practical matter, sanctions on these particular regions of Ukraine present substantial compliance challenges, very similar to those seen in Crimea, as U.S., EU, and UK persons are again prohibited from engaging in transactions involving regions that are not internationally recognized states. Moreover, the precise boundaries of the sanctioned regions are unsettled. The U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") has indicated in published guidance that the DNR and the LNR do not presently encompass the entire Ukrainian oblasts, or provinces, of Donetsk and Luhansk. Similarly, EU restrictions cover areas of the relevant oblasts which are not under the control of the Ukrainian authorities. The United Kingdom, on the other hand, relies on the territorial definition outlined in Decree Number 32/2019 issued by the President of Ukraine. It is also conceivable that the "Covered Regions" could in future be extended to include some or all of the Zaporizhzhia and Kherson regions of Ukraine that Russia purported to annex in September 2022, in line with the European Union's approach. For purposes of determining whether a particular location in eastern Ukraine is within the Covered Regions—and is therefore subject to comprehensive U.S. sanctions—OFAC has not yet publicly delineated the borders of those regions, but has offered that "U.S. persons may reasonably rely on vetted information from reliable third parties, such as postal codes and maps." Importantly, as of this writing, the Russian Federation is *not* subject to comprehensive sanctions. That is, U.S. persons are prohibited from engaging in substantially all transactions involving only a small number of jurisdictions, namely Cuba, Iran, North Korea, Syria, and the Crimea, Donetsk People's Republic, and Luhansk People's Republic regions of Ukraine. The remaining U.S. sanctions programs, and all EU and UK sanctions programs, including sanctions targeting Russia, are generally list-based—meaning that U.S. persons are restricted from engaging in certain transactions involving certain specified parties, as well as those parties' direct and indirect majority-owned entities (or, in the case of the European Union and United Kingdom, those parties' direct and indirect majority-owned and/or controlled entities). That said, as discussed below, the number of Russia-related parties that are subject to list-based sanctions exploded during 2022 and is poised for further growth during the year ahead. **B. Sectoral Sanctions** In addition to the comprehensive sanctions on the DNR and LNR discussed above, an unusual feature of the sanctions programs targeting Russia are the sectoral sanctions, under which it is prohibited to engage in certain narrow types of activities with certain designated entities, as set forth on the Sectoral Sanctions Identifications ("SSI") List or the Non-SDN Menu-Based Sanctions ("NS-MBS") List administered by OFAC and the equivalent lists maintained by other key allies, including the European Union and the United Kingdom. This type of sectoral designation limits the types of interactions a targeted entity is allowed to undertake with U.S., EU, and UK persons pursuant to a series of OFAC "Directives" and EU and UK regulations that for nearly a decade have targeted Russia's financial, energy, defense, and oil industries. Underscoring the narrow scope of the sectoral sanctions on Russia, OFAC expressly provides that, absent some other prohibition, all other lawful U.S. nexus dealings involving a targeted entity are permitted. That same approach in relation to sectoral sanctions has been adopted in the European Union and the United Kingdom. Immediately following Russia's invasion of Ukraine, the Biden administration announced four new sectoral sanctions Directives that bar U.S. persons from engaging in certain dealings involving

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

some of the Russian Federation's most economically consequential institutions. Those restrictions were paralleled by the European Union and the United Kingdom. In particular, the measures restrict Russia's access to capital by:

- Prohibiting U.S. financial institutions from participating in the primary or secondary market for "new" bonds issued by Russia's central bank, finance ministry, and principal sovereign wealth fund (collectively, the "Russian Sovereign Entities");
- Prohibiting U.S. financial institutions from opening or maintaining a correspondent or payable-through account for or on behalf of, or processing a transaction involving, ***Sberbank*** or any of its majority-owned entities, thereby cutting off Russia's largest bank from the U.S. financial system;
- Prohibiting U.S. persons from dealing in "new" debt or "new" equity of 13 major Russian state-owned enterprises and financial institutions, further limiting Russia's ability to raise new capital for its military activities in Ukraine; and
- Prohibiting U.S. persons, except as authorized by OFAC, from engaging in any transaction involving the three named Russian Sovereign Entities, including any transfer of assets to such entities or any foreign exchange transaction for or on behalf of such entities. This novel sectoral sanctions measure, together with similar restrictions by each member of the Group of Seven ("G7"), has proven especially impactful. While neither the Russian Central Bank, the Russian National Wealth Fund, nor the Russian Ministry of Finance are blocked, using this unique tool the allies effectively immobilized around $300 billion in international reserves that the Russian government had stockpiled to insulate its economy from the effects of sanctions.

During the war's opening days, the European Union, in another highly impactful move, directed the Belgium-based ***Society for Worldwide Interbank Financial Telecommunication*** ("SWIFT") to deny select Russian banks access to its financial messaging services, which serve as the principal means for global financial institutions to send and receive transaction-related information. The coalition's early use of sectoral sanctions, which we discuss in depth in a previous client alert, was animated by a policy interest in imposing tangible costs on the Kremlin for invading Ukraine, while minimizing the collateral consequences of targeting one of the world's largest and (then) most interconnected economies. As the war in Ukraine has stretched on, the allies have demonstrated an increasing willingness to impose a variety of severe restrictions on Russia, including the expansive use of blocking sanctions. **C. Blocking Sanctions** Since February 2022, the United States, the European Union, and the United Kingdom, in a historic burst of activity, have each added approximately 1,500 new Russia-related individuals and entities to their respective consolidated lists of sanctioned persons. While the lists do not always overlap, increasing the compliance burden on multinational companies, the level of coordination among the allies has been particularly impactful. As an example of the sweeping nature of the new designations, in the United States, of all the parties that have been named to OFAC's Specially Designated Nationals and Blocked Persons ("SDN") List over the decades, around one in ten were designated in just the past year for their activities involving Russia. Blocking sanctions are arguably the most potent tool in a country's sanctions arsenal, especially for countries such as the United States with an outsized role in the global financial system. Upon becoming designated an SDN (or other type of blocked person), the targeted individual or entity's property and interests in property that come within U.S. jurisdiction are blocked (i.e., frozen) and U.S. persons are, except as authorized by OFAC, generally prohibited from engaging in transactions involving the blocked person. The same applies to persons designated by the European Union or the United Kingdom. The SDN List, and its EU and UK equivalents, therefore function as the principal sanctions-related restricted party lists. The effects of blocking sanctions often reach beyond the parties identified by name on these lists. By operation of OFAC's Fifty Percent Rule (and in the EU and the UK, the ownership and control test), restrictions generally also extend to entities owned 50 percent or more in the aggregate by one or more blocked persons (or, in the case of the EU and UK, to entities owned more

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

than 50 percent or controlled by a blocked person, with the EU indicating that aggregation is possible), whether or not the entity itself has been explicitly identified. During 2022, the allies repeatedly used their targeting authorities to block Russian political and business elites, as well as substantial enterprises in sectors such as banking, energy, defense, aerospace, and mining seen as critical to financing and sustaining the Kremlin's war effort. Notable designations included:

- Government officials, including President Vladimir Putin, as well as Russia's foreign minister, defense minister, central bank chief, and 328 members of the Russian State Duma. Belarus's President Alyaksandr Lukashenka was also re-designated after permitting Russian troops to launch attacks on Ukraine from Belarusian soil;
- Prominent Russian oligarchs such as Alisher Usmanov and Vladimir Potanin and, in the European Union and the United Kingdom, Roman Abramovich;
- Major financial institutions, including ***VTB Bank*** and Sberbank, that together represent around 80 percent of Russia's banking sector by assets;
- Energy firms, including ***Nord Stream 2 AG***, the Swiss company in charge of developing a new gas pipeline between Germany and Russia; while Germany has suspended the approval process for Nord Stream 2 (disallowing its operation), notably the European Union and the United Kingdom have not followed the United States in designating Nord Stream 2 AG;
- Defense and aerospace firms, including the state-owned defense conglomerate ***Rostec*** and the mercenary group ***Private Military Company Wagner***, which have been instrumental in equipping and manning Russia's military operation in Ukraine; and
- Extractive firms such as ***Alrosa***, the world's largest diamond mining company and a major source of revenue for the Russian state.

Many of those U.S. designations were made under the authority of Executive Order 14024 , which we discussed in depth in a previous client alert. Importantly, E.O. 14024 authorizes blocking sanctions against persons determined to operate in certain sectors of the Russian economy determined by the Secretary of the Treasury. Underscoring the uncertain business environment in Russia, parties in multiple sectors now operate under the threat of being added to the SDN List, including those operating in the technology, defense and related materiel, financial services, aerospace, electronics, marine, accounting, trust and corporate formation services, management consulting, or quantum computing sectors of Russia's economy. Moreover, OFAC has indicated that it is prepared to use its authorities to impose blocking sanctions on any non-U.S. persons otherwise involved in circumventing U.S. sanctions, solidifying Russia's grasp on occupied regions of eastern Ukraine, or arming, equipping, or materially supporting the Russian military. **D. Export Controls** In addition to economic and financial sanctions, the United States and its allies rapidly expanded their export control regimes targeting Russia and Belarus in response to Moscow's further invasion of Ukraine and Belarus's support of the effort. Significantly, the U.S. Department of Commerce's Bureau of Industry and Security ("BIS") imposed a license requirement on all controlled dual-use items subject to its jurisdiction when destined for, reexported to, or transferred within Russia or Belarus. In tandem with this action, BIS expanded the scope of U.S. licensing requirements on *foreign-produced* items exported, reexported, or transferred within Russia or Belarus in a range of circumstances, such that:

- Foreign-made items that incorporate more than 25 percent controlled U.S.-origin content are subject to BIS's export licensing regime under the traditional application of the *de minimis* rule;
- Foreign-made items that are the "direct product" of controlled U.S.-origin technology or software, or of a manufacturing facility or equipment derived from such controlled U.S. technology or software, and are items of a kind described on

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

the S. Commerce Control List (i.e., not EAR99 items), or are items that could be used in identified industrial sectors, are subject to an export license requirement when destined for any person in Russia or Belarus;

- Foreign-made items that would be designated EAR99 (i.e., generally not controlled) and are a "direct product" of controlled U.S.-origin technology or software, or a manufacturing facility or equipment derived from such controlled technology or software, are subject to an export license requirement when destined for any Russian or Belarusian military end user identified on the Entity List ; and
- With respect to both of those new foreign direct product rules, items produced in a partner country that has implemented substantially similar export controls on Russia and Belarus are exempt from the U.S. license requirement in order to avoid duplicate licensing efforts.

Further, BIS expanded the scope of pre-existing prohibitions related to military end users and military end uses in Russia and Belarus to cover *any* item subject to the U.S. Export Administration Regulations ("EAR"), including items "subject to the EAR" by operation of one of the foreign direct product rules described above. The controls described above produced immediate impacts as Russia's military, absent new shipments of advanced technology, reportedly was forced to retrieve low-end semiconductors from household appliances such as dishwashers and refrigerators. For a more detailed discussion of those controls, please see our February 2022 client alert. BIS also expanded the scope of its licensing control to include EAR99 items—that is, items that are *not* described by an Export Control Classification Number ("ECCN") on the EAR's Commerce Control List—for Russia and Belarus. These controls largely parallel EU controls on certain targeted goods, equipment, parts, and materials for use in significant industry sectors, including oil refining (in addition to pre-existing controls on items used in oil and gas exploration and production), industrial and manufacturing activities, production of chemical and biological agents, quantum computing, and advanced manufacturing. In addition, BIS published rules to implement a ban on "luxury goods" destined for Russia or Belarus or to sanctioned Russian or Belarusian oligarchs, regardless of their location. The European Union and the United Kingdom have followed a similar approach, though the lists of goods targeted differ between jurisdictions. In general terms, the EU and UK lists are organized under broad headings such as "goods which may enhance Russia's military and technological advancement," "goods that may enhance Russia's industrial capabilities," or "critical industry goods." The expansive headings allow the European Union and the United Kingdom to include numerous groups of seemingly unrelated items within their restrictions, adding to the complexity of these measures. The United States has also prohibited the exportation, reexportation, sale, or supply from the United States, or by a U.S. person, of U.S. Dollar-denominated banknotes to the Government of the Russian Federation or any person located in the Russian Federation. The European Union and the United Kingdom have imposed equivalent restrictions on the export of Euro and Sterling banknotes, respectively. As a general matter, export license applications under the new export controls on Russia and Belarus will, except in limited circumstances, be reviewed subject to a policy of denial, essentially imposing an embargo on all U.S.-origin dual-use items, items produced with dual-use software and technology, and a broad range of non-dual-use items used in multiple industrial sectors, for Russia and its cooperating neighbor. EU and UK authorities have taken a similar approach. Of particular note is BIS's aggressive use of export controls to target the Russian and Belarusian commercial aviation sectors. In light of the wide-ranging use of U.S.-origin parts, equipment, and technology in commercial aviation applications, expanded U.S. export controls have cut off many private and commercial aircraft owned, leased, or operated by Russian or Belarusian persons from transiting to or from those countries or receiving parts or services provided by U.S. persons. In addition, BIS has responded to the Russian government's effective nationalization of hundreds of U.S. and European aircraft by issuing temporary denial orders against major Russian airlines and by publishing lists of aircraft that have been flown in violation of U.S. export controls, rendering transactions involving either subject to expansive prohibitions. The EU and UK restrictions on aviation and space

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

goods and technology have added to the logistical complexities facing the aviation sector, and have been further exacerbated by prohibitions on Russian owned, registered, controlled, or chartered aircraft entering or leaving EU and UK airspace. To encourage compliance and identify potential evasion of the new rules described above, BIS and the U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") in June 2022 issued a first-of-its-kind joint alert to financial institutions urging them to apply heightened due diligence to transactions with a higher risk of facilitating export control evasion. The joint alert includes a list of commodities that BIS has identified as presenting special concern because of their potential diversion to military applications in Russia and Belarus, including aircraft parts, cameras, global positioning systems, integrated circuits, oil field equipment, and related items, as well as a list of transshipment hubs that present diversion risks to Russia and Belarus. It also highlights transactional "red flags" that are useful both to financial institutions and other industry participants. **E. Import Prohibitions** In addition to restricting exports to Russia, starting in March and April 2022 the United States, the European Union, and the United Kingdom banned the importation of certain Russian-origin goods—principally those consisting of items closely associated with Russia or that have the potential to generate hard currency for the Kremlin. The Biden administration first used this particular policy tool by barring imports into the United States of certain energy products of Russian Federation origin, namely crude oil, petroleum, petroleum fuels, oils, and products of their distillation, liquified natural gas, coal, and coal products. Intending to limit Russian revenue without driving up global energy prices, OFAC published guidance noting that Russian-origin energy products other than those specified in Executive Order 14066 remain potentially eligible for importation into the United States. OFAC further indicated that, absent some other prohibition, such as the involvement of a blocked person, non-U.S. persons would not risk U.S. sanctions liability for continuing to import Russian-origin energy products into third countries that have not imposed such an import ban. As Russia's war in Ukraine continued, the Biden administration subsequently barred the importation into the United States of Russian Federation origin fish, seafood, alcoholic beverages, non-industrial diamonds, and eventually gold. As with other Russia-related sanctions authorities, the Secretary of the Treasury has broad discretion under Executive Order 14068 to, at some later date, extend the U.S. import ban to additional Russian-origin products. While U.S. imports from Russia historically have been minimal, the same is not true for the European Union and the United Kingdom. Consequently, for the restrictions to be meaningful, the EU and UK import measures have had to be similarly broad—and they are. The European Union has banned coal, crude oil and petroleum products, iron and steel products, gold and the broad category of "revenue-generating goods," which is a catch-all for any other items the European Union may want to restrict. The United Kingdom has prohibited the import of arms and related materiel, iron and steel products, oil and oil products, coal and coal products, liquified natural gas, gold, gold jewelry, and processed gold. However, there remain significant differences between the transatlantic partners in this regard, reflecting their different ranges of independence from the Russian economy and its energy sector. Notably, the European Union and the United Kingdom have not yet restricted the import of Russian liquified natural gas. EU Member States such as Hungary, Bulgaria, Croatia, and Czechia also negotiated exceptions to the prohibitions described above, the most notable of which has the effect of excluding crude oil delivered by pipeline from the import ban. Furthermore, highlighting the degree of bipartisan support for limiting Russia's access to the U.S. market, the U.S. Congress in April 2022 enacted legislation codifying into law the Biden administration's Russian oil import ban, as well as suspending the United States' permanent normal trade relations with Russia and Belarus, thereby exposing products originating from those two countries to increased U.S. tariffs. Similarly, the European Union and the United Kingdom have revoked Russia's most favored nation trading status, triggering higher tariffs. **F. New Investment Prohibitions** In parallel with efforts to restrict Russian imports into the United States, and drawing on many of the same legal authorities, the Biden administration during March and April 2022 also imposed a series of progressively broader prohibitions on new investment in the Russian Federation. Specifically, President Biden in quick succession signed three separate Executive Orders prohibiting U.S. persons, wherever located, from making a "new investment" in the energy sector in the Russian Federation (E.O. 14066), then in any other sector of the Russian

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

Federation economy as may be determined by the Secretary of the Treasury (E.O. 14068), and eventually on April 6, 2022 in *all* sectors of the Russian Federation economy (E.O. 14071). By encompassing the entire Russian economy, the last of those three Executive Orders in effect swallows the other two. In a sign of the blistering pace at which new trade restrictions on Russia were being rolled out during the war's earliest phases, the business community had to wait two months after the Biden administration's banning of all "new investment" for guidance as to what "new investment" entails. OFAC was operating at a high cadence in rolling out new actions and did not have the bandwidth to immediately provide the guidance, frequently asked questions ("FAQs"), and other documentation that typically accompany such meaningful new measures. In a set of FAQs released on June 6, 2022, OFAC for the first time detailed how the agency understands what does (and does not) constitute a prohibited new investment in Russia. Broadly speaking, OFAC considers "new investment" to mean a U.S. person making a commitment of capital or other assets, on or after the effective date of the relevant Executive Order (in most cases, April 6, 2022), for the purpose of generating returns or appreciation within the Russian Federation. OFAC interprets Executive Order 14071 as prohibiting U.S. persons from, among other things, purchasing both new and existing debt and equity securities issued by any entity located in the Russian Federation—regardless whether the issuer is subject to blocking or sectoral sanctions and regardless when the debt or equity was issued. OFAC has further indicated that E.O. 14071 prohibits U.S. persons from purchasing debt and equity securities issued by any entity located outside of Russia that has certain close ties to Russia such as deriving 50 percent or more of its revenues from investments inside the Russian Federation. Crucially, however, OFAC has advised that the agency generally does not view the new investment prohibition as applying to ordinary course commercial transactions involving Russia, including exports or imports of goods, services, or technology, or related sales or purchases. Notably for multinational enterprises, U.S. persons may continue to fund, but not expand, their existing subsidiaries and affiliates located in Russia. U.S. persons may continue to hold previously acquired securities of non-sanctioned Russian issuers and may also divest such securities, subject to certain conditions. Such divestment transactions are potentially permissible, provided that the transaction does not involve a blocked person, the ultimate buyer is a non-U.S. person, and the transaction is not otherwise prohibited by OFAC. Notwithstanding those and other exceptions, the U.S. prohibition on new investment in the Russian Federation further complicates an already challenging local business environment and, by barring new or expanded operations, is likely to encourage multinational companies' continued flight from Russia. This self-sanctioning by private actors was not a part of the well-laid sanctions plan that the coalition developed in the run-up to the February 2022 attack. Indeed, in recent weeks, the United States especially has redoubled efforts to emphasize that it desires certain businesses to remain in Russia despite the breadth of sanctions and related restrictions. The United Kingdom's approach to investment restrictions has been equally broad, while the European Union has taken a more limited approach of strictly banning investment in the energy sector in Russia, as well as the Russian mining and quarrying sector, while carving out exceptions for certain raw materials. **G. Services Prohibitions** As the Kremlin's war in Ukraine stretched on, the United States, the European Union, and the United Kingdom in May and September 2022 reached deeper into their respective policy toolkits to ban the exportation to Russia of certain professional and technological services. Executive Order 14071—the broad and flexible legal authority that underpins many of the U.S. Government's later trade restrictions on Russia—prohibits the exportation from the United States, or by a U.S. person, of any category of services as may be determined by the Secretary of the Treasury, to any person located in the Russian Federation. Acting pursuant to that authority, the United States during 2022 barred U.S. exports to Russia of accounting, trust and corporate formation, and management consulting services, as well as quantum computing services. The rationale for targeting those particular services—the provision of which is also potentially grounds for designation to the SDN List—appears to be a U.S. policy interest in denying Moscow access to services with the potential to enable sanctions evasion or bolster the Russian military. Although the U.S. services bans contain exceptions, such as permitting the provision of services to entities located in Russia that are owned or controlled by U.S. persons, OFAC otherwise interprets those measures in a

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

very broad manner. For example, the agency has noted that, for the purposes of E.O. 14071, the term "accounting services" includes "services related to the measurement, processing, and evaluation of financial data about economic entities." The term "management consulting services" includes, among other activities, "services related to strategic business advice." In light of the prohibitions' seemingly unbounded reach, many leading professional services firms—whose offerings are key to operating a multinational business—have opted to withdraw from the Russian market rather than risk triggering U.S. sanctions. The European Union and the United Kingdom have imposed equally wide-ranging services prohibitions. The European Union has restricted the provision of accounting, auditing, bookkeeping and tax consulting, business and management consulting, public relations, information technology consulting, architectural and engineering, legal advisory, market research, public opinion polling, advertising, and technical testing and analysis services. Both jurisdictions also restricted trust and corporate formation services—which have historically been key tools for wealthy Russians to shield their assets. Despite core similarities across the three jurisdictions, important different exceptions apply. Most notably, the European Union allows for these services to be provided to Russian entities that are owned by, or solely or jointly controlled by, an entity incorporated under the laws of an EU or European Economic Area Member State, Switzerland, the United Kingdom, the United States, South Korea, or Japan. Meanwhile, the United Kingdom allows for certain exceptions in relation to compliance with UK statutory or regulatory obligations. Within the financial services sector, the United Kingdom prohibited its financial institutions from establishing correspondent banking relationships with designated persons, and proceeded to designate all major Russian banks. To further tighten access to its financial infrastructure, the European Union implemented restrictions relating to deposits being held by EU credit institutions, such that Russian natural or legal persons and entities directly or indirectly owned more than 50 percent by them cannot make deposits greater than 100,000 Euros. A prohibition on the provision of crypto-asset wallet, account, or custody services, regardless of the value of the assets, also applies in the European Union. The United Kingdom has not implemented equivalent measures, but it has subjected crypto-asset exchange providers and custodian wallet providers to strict reporting obligations. In late 2022 and early 2023, the allies also introduced new and ambitious forms of services bans, discussed more fully below, designed to cap the price of seaborne Russian crude oil and petroleum products. **H. Price Cap on Crude Oil and Petroleum Products** To minimize the Kremlin's ability to profit from surging energy prices stemming from its invasion of Ukraine, the G7 countries in September 2022 committed to impose a novel measure to squeeze Russia's chief source of revenue—a price cap on Russian-origin crude oil and petroleum products. Effective December 5, 2022, the United States, Canada, France, Germany, Italy, Japan, and the United Kingdom, alongside the European Union and Australia (collectively, the "Price Cap Coalition"), prohibited the provision of certain services that support the maritime transport of Russian-origin crude oil from Russia to third countries, or from a third country to other third countries, unless the oil has been purchased at or below a specified price. A separate price cap with respect to Russian-origin petroleum products became effective on February 5, 2023. The types of services that are potentially restricted varies modestly among the Price Cap Coalition countries, but generally includes activities such as brokering, financing, and insurance. A detailed analysis of the price cap, and how it is being implemented by key members of the Price Cap Coalition, can be found in our previous client alert. From a policy perspective, the price cap is intended to curtail Russia's ability to generate revenue from the sale of its energy resources, while still maintaining a stable supply of these products on the global market. The measure is also designed to avoid imposing a blanket ban on the provision of *all* services relating to the transport of Russian oil and petroleum products, which could have far-reaching and unintended consequences for global energy prices. Accordingly, the price cap functions as an exception to an otherwise broad services ban. Best-in-class maritime service providers, which are overwhelmingly based in Price Cap Coalition countries, are permitted to continue supporting the maritime transport of Russian-origin oil and petroleum products, but only if such oil or petroleum products are sold at or below a certain price. In order to steer clear of a potential enforcement action, service providers from Price Cap Coalition countries that deal in seaborne Russian oil or petroleum products will need to be able to provide certain evidence that the price cap was not breached in

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

regard to the shipment that they are servicing. For example, the United States, United Kingdom, and European Union have each set forth a detailed attestation process by which maritime transportation industry actors can benefit from a "safe harbor" from prosecution arising out of violations by third parties. By obtaining price information or an attestation from relevant counterparties, ship owners, charterers, insurers, financial institutions, and others throughout the maritime supply chain may substantially mitigate their risk of non-compliance arising out of misrepresentations or evasive actions taken by third parties in violation of the price cap programs. Relevant authorities in those three jurisdictions have indicated that compliance with the recordkeeping and attestation framework will generally shield a service provider from the otherwise strict liability regime. It remains to be seen whether other countries will eventually join the Price Cap Coalition or agree to implement similar restrictions in the future, which could create additional complexity in the global energy supply chain where Russian-origin oil or petroleum products are involved. As of this writing, the price cap seems to be having a modest impact on Russian oil revenues. In setting the initial price cap on Russian-origin crude oil at $60 per barrel—above the prevailing market price for Russian Urals—policymakers appear to have offered maritime service providers a gentle introduction to a novel and complex policy instrument. As market participants become more familiar with the mechanics of the price cap, the Price Cap Coalition may periodically ratchet down the relevant price caps to further squeeze Russian energy revenue. **I. Possible Further Trade Controls on Russia** Although leading democracies during 2022 introduced a dizzying array of trade restrictions on Russia, the coalition has not yet exhausted its policy toolkit. The allies could, in coming months, further increase pressure on the Kremlin by imposing blocking sanctions on yet more Russian banks and Russian elites, including especially oligarchs whose vast business interests may offer inviting targets. In the event of a substantial new provocation by Moscow, it is not out of the question that the Biden administration could follow the model developed in Venezuela by imposing blocking sanctions on the entirety of the Government of the Russian Federation. Officials in Washington and Brussels have also begun to weigh how to fund Ukraine's eventual reconstruction. Building on initiatives such as the U.S. Department of Justice's Task Force KleptoCapture and the multilateral Russian Elites, Proxies, and Oligarchs Task Force, which are pursuing seizure and forfeiture of certain assets belonging to sanctioned parties if they meet legal standards beyond the fact that they are sanctioned, the United States could potentially move to deploy forfeited Russian assets to aid Kyiv. Similarly, the European Commission has been exploring options to pay for the reconstruction of Ukraine with investment proceeds derived from Russian assets currently frozen in the European Union. As we have noted elsewhere, in the United States any effort to redirect private assets—or, more controversially, Russian sovereign assets—would likely require an act of Congress to reduce the not insignificant legal difference and distance between sanctions and seizures, suggesting that any such initiative is unlikely to materialize in the near term. Finally, the United States, the European Union, and the United Kingdom have so far resisted calls to label Russia a state sponsor of terrorism, or, in the case of the United States, to impose secondary sanctions, citing the risk of fracturing the coalition by penalizing companies based in allied jurisdictions for their dealings involving Russia. The European Parliament has called on EU Member States to work toward the introduction of a legal framework to designate state sponsors of terrorism, so that Russia can be so designated. As noted above, the United States and its allies, while imposing extensive restrictions on Moscow, have also stopped short of comprehensive sanctions and export controls like the U.S. measures that presently apply to Cuba, Iran, North Korea, Syria, and certain Russian-occupied regions of Ukraine. Although those sorts of draconian restrictions do not appear to be imminent, the United States and its allies could quickly reconsider such measures in the event of a complete breakdown in relations with Moscow—for example, if the Kremlin were to use nuclear weapons in Ukraine. **II. U.S. Trade Controls on China** Russia's invasion nearly overshadowed what otherwise would have been the principal trade story of the year: continuing high tensions between Washington and Beijing. During 2022, the Biden administration deployed both traditional and innovative trade restrictions to counter China's continued troubling activities at home and worrying ambitions abroad. In the U.S. National Security Strategy released in October 2022, the Biden administration squarely addressed the ongoing geopolitical competition between the United States and China,

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

labeling Beijing "the only competitor with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to advance that objective." This stark characterization reflects an emerging bipartisan consensus among top U.S. officials and most members of Congress that China represents a "pacing challenge" to certain U.S. national interests, particularly technological leadership. In a sea change from longstanding U.S. aversion to state industrial policy, the United States over the past year embraced a protectionist-leaning "modern industrial and innovation strategy" to counteract China's influence on the world stage, including through:

- The promulgation of import restrictions on Chinese goods linked to forced labor;
- The passage of multiple legislative packages to incentivize U.S. technological competitiveness;
- The imposition of sweeping export controls on certain advanced integrated circuits, semiconductor manufacturing equipment, and supercomputers involving China;
- The furthering of multilateral efforts to limit China's technological capabilities; and
- The continuation and enhancement of scrutiny of proposed Chinese investments in the United States.

A. Uyghur Forced Labor Prevention Act The Uyghur Forced Labor Prevention Act ("UFLPA") was enacted in December 2021 to deny certain goods produced in China's Xinjiang Uyghur Autonomous Region ("Xinjiang") access to the U.S. market, primarily through the imposition of a rebuttable presumption that all goods mined, produced, or manufactured even partially within Xinjiang are the product of forced labor and are therefore not entitled to entry at U.S. ports. This rebuttable presumption took effect on June 21, 2022. Throughout the second half of 2022, vigorous enforcement of the UFLPA by U.S. Customs and Border Protection ("CBP")—which is a unit of the U.S. Department of Homeland Security—led to a substantial volume of goods being denied clearance at various U.S. ports as many suppliers scrambled to trace complete supply chains to ensure compliance. Guidance released by CBP in June 2022 highlighted cotton, tomatoes, and polysilicon as high-priority sectors for enforcement, but CBP's targeting has since expanded to include products that incorporate polyvinyl chloride (commonly known as PVC) and aluminum—with the latter a precursor to potentially restricting the import of automobile parts. The U.S. Department of Homeland Security has also named over 30 entities to its UFLPA Entity List, as a result of which those entities' products and services are presumed to be made with forced labor and are prohibited from entry into the United States. As described in more detail in our 2021 Year-End Sanctions and Export Controls Update, as well as a separate June 2022 client alert, importers of any products that may be suspected to incorporate inputs sourced from Xinjiang, from any entity listed on the UFLPA Entity List, or from companies participating in any one of several of China's "anti-poverty alleviation" programs should be aware of the new supply chain tracing requirements necessary to demonstrate that the imports are not subject to the rebuttable presumption. **B. Technological Competitiveness Legislation** Alongside efforts to restrict imports that present potential human rights concerns, a key pillar of the Biden administration's trade policy with respect to China has involved a turn inward by the United States and toward a nationalist industrial policy, including directly subsidizing industries critical to U.S. supply chains and national security. Consistent with the White House's National Security Strategy—which describes strategic public investment as "the backbone of a strong industrial and innovation base in the 21st century global economy"—the U.S. Congress during 2022 adopted two massive legislative packages that, among other things, direct billions of dollars toward boosting domestic manufacturing. The CHIPS and Science Act (the "CHIPS Act"), signed into law by President Biden in August 2022, took significant steps—including authorizing $280 billion in spending—to address underlying national security concerns regarding the longstanding offshoring of critical technological capabilities, a situation that was highlighted during the pandemic which saw significant supply chain disruptions (in part because of China's "Zero COVID" policy), and which exacerbated the fact that almost all personal protective equipment the United States needed was made in China. In addition to incentivizing investment in U.S. semiconductor

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

manufacturing through more than $50 billion of direct government subsidies, the CHIPS Act also includes guardrails to prevent U.S. companies that receive subsidies under the Act from engaging in significant transactions involving "the material expansion of semiconductor manufacturing capacity in the People's Republic of China or any other foreign country of concern." This legislation marked a historic departure for the U.S. Government, which until recently had not significantly restricted private companies' strategies for offshoring and outsourcing technology outside traditional export control regimes. Following passage of the CHIPS Act, major semiconductor makers quickly broke ground on new facilities located in the United States. That same month, President Biden signed into law the Inflation Reduction Act of 2022 to boost domestic energy production and manufacturing, as well as to provide direct funding to support the transition to renewable energy sources and to secure domestic energy supply chains. In an effort to relocate electric-vehicle supply chains from China to the United States, the Inflation Reduction Act includes billions of dollars in subsidies for electric vehicles assembled in North America—a move that has rankled close U.S. allies in Europe who roundly have criticized the measure as protectionist and discriminatory against European goods. The European Commission in January 2023 released its Green Deal Industrial Plan, building on the pre-existing RePowerEU initiative and the European Green Deal, to enhance the competitiveness of Europe's net-zero industry. We expect that the EU response to the Inflation Reduction Act will be further developed during 2023. In September 2022, President Biden signed an Executive Order directing the investment of another $2 billion into strengthening domestic biotechnology and biomanufacturing supply chains through the National Biotechnology and Biomanufacturing Initiative, further exemplifying the current administration's approach to identifying and directly supporting supply chains across various industries deemed critical for national security. **C. Export Controls**

1. Controls on Advanced Computer Chips

Controlling the manufacture, supply, and export of certain advanced technologies has become a core feature of the U.S. Government's evolving trade policy toward Beijing. As we discuss in a recent article, the U.S. Government has over the past year employed a variety of methods to strengthen control over strategic supply chains and to limit the export of these key technologies to strategic competitors, including China. Consistent with its traditional authorities, BIS on August 15, 2022 issued an interim rule to implement new controls on four so-called Section 1758 technologies—named after the section of the Export Control Reform Act of 2018 that tasked the agency with regulating emerging and foundational technologies. As discussed in Section IV.A, below, that measure imposes new restrictions on certain ultra-wide bandgap semiconductors and certain emerging electronic computer aided design software. Both of these restrictions were imposed in a clear effort to limit the ability of U.S. adversaries to produce advanced technologies. Also in August 2022, BIS used the "is informed" provision of the Military End Use / User ("MEU") Rule to, without any formal rulemaking process, privately inform parties that a license is required for exports of specified items due to an "unacceptable risk of use in or diversion to a 'military end use' or a 'military end user.'" A party that receives such a notice is prohibited from exporting the specified items to destination countries identified in the notice without BIS licensing, and such export license applications are subject to a presumption of denial. News reports indicate that BIS leveraged that little-used regulatory provision to, on short notice, restrict at least two U.S.-based semiconductor companies from exporting to China and Russia certain advanced integrated circuits and associated technology commonly used in sophisticated artificial intelligence applications over concerns that the chips could be diverted to a military end use or end user. Although BIS maintains a policy of not publicly commenting on such restrictions on private parties, these sudden and closely targeted controls led observers to speculate that further restrictions were close at hand.

2. Controls on Advanced Computing Integrated Circuits, Semiconductor Manufacturing Equipment, and Certain Items Used to Develop Supercomputers

On October 13, 2022, BIS announced groundbreaking and far-reaching controls on

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

advanced computing integrated circuits (“ICs”), computer commodities that contain such ICs, and certain semiconductor manufacturing items destined for China. As discussed at length in our recent client alert, these new regulations appear calculated to create an effective embargo against providing to China the technology, software, manufacturing equipment, and commodities that are used to make certain advanced computing ICs and supercomputers; to curtail China’s use of these targeted items in the development of weapons of mass destruction, artificial intelligence, supercomputing-enhanced war fighting, and technologies that enable violations of human rights; and to combat China’s “military-civil fusion” development strategy. These complex regulations caused significant upheaval in the affected industries as they were implemented over a two-week period in October 2022 and increased the prospect of other potential efforts to decouple advanced technology supply chains that still link the United States and China. At the heart of these new export controls is BIS’s addition to the Commerce Control List of new and revised Export Control Classification Numbers. These new ECCNs control certain semiconductor manufacturing equipment and specially designed parts, components, and accessories; specified high-performance ICs; certain computers, electronic assemblies, and components containing such ICs; and associated software and technology. The accompanying new Regional Stability (“RS”) controls apply specifically to these goods when they are destined for the People’s Republic of China (“PRC”)—a destination control that now also includes Hong Kong and, as of January 17, 2023, Macau. Separately, new Antiterrorism (“AT”) controls were also announced at the same time, which further restrict the export of these commodities and associated technology to such highly controlled destinations as Iran, North Korea, and Syria. BIS also introduced two new foreign direct product (“FDP”) rules and expanded another. Foreign direct product rules expand the scope of U.S. export controls to certain foreign-produced items that are derivative of specified U.S. software and technology. The contours of each FDP rule are unique, but in the case of the new rules targeting China, the FDP rules have been expanded to effectively cut off China’s access to certain foreign-produced advanced ICs, semiconductor manufacturing equipment, and items used to develop and maintain supercomputers. The new advanced computing FDP rule brings within the scope of U.S. export controls certain foreign-produced advanced computing items destined for the PRC, as well as certain technology developed by an entity headquartered in the PRC for the production of a mask or an IC wafer or die. Similarly, the new supercomputer FDP rule expands U.S. export controls to certain foreign-produced items used in the design, development, production, operation, installation (including on-site installation), maintenance (checking), repair, overhaul, or refurbishing of a “supercomputer“ (as specifically defined within the regulations) located in or destined for the PRC, in addition to any such items that will be incorporated into or used in the development or production of parts, components, or equipment that will eventually be used in a supercomputer located in or destined for the PRC. Importantly, the current definition of “supercomputer” captures certain data centers that meet the definitional parameters, exemplifying the broad scope of these new controls. Finally, the new controls expand the pre-existing Entity List FDP rule —originally aimed at restricting the flow of certain foreign-produced items to ***Huawei*** and its affiliates—to restrict certain foreign-produced items to an additional 28 China-based entities already designated to the Entity List over the past several years for their alleged participation in nuclear and other weapons of mass destruction proliferation, as well as surveillance and other human rights abuses. New license requirements are also in place for certain items that fall under U.S. export controls for which the exporter has knowledge (defined to cover actual knowledge and an awareness of a high probability, which can be inferred from acts constituting willful blindness) that the item will be used in certain activities (1) associated with the development or maintenance of a “supercomputer” in or destined for China, or associated components or equipment, or (2) destined for end use in semiconductor fabrication facilities in China that fabricate certain ICs (or for which the exporter does not know if the facility manufactures the specified ICs). The ICs specifically targeted by these new restrictions are some of the most advanced ICs presently in existence, including: (1) logic integrated circuits using a non-planar transistor architecture or with a production technology node of 16/14 nanometers or less; (2) NOT AND (“NAND”) memory integrated circuits with 128 layers or more; and (3) dynamic random-access memory (“DRAM”) integrated circuits using a production technology node of

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

18 nanometer half-pitch or less. Perhaps the most far-reaching feature of these new export controls are the restrictions BIS has placed on the activities of U.S. persons, even when their activities do not involve controlled U.S.-origin items. Broadly speaking, U.S. persons, including dual nationals and lawful permanent residents of the United States, wherever located, must now apply for licenses to facilitate or engage in shipping, transmitting, or transferring to or within China certain items that are not otherwise captured under U.S. export controls as follows:

- **Prohibition Category 1**: Any item not "subject to the EAR" that the individual or entity knows will be used in the development or production of ICs at a semiconductor fabrication facility located in China that fabricates certain ICs such as advanced logic, NAND, and DRAM ICs; or in the servicing of any such items;
- **Prohibition Category 2**: Any item not subject to the EAR and meeting the parameters of any ECCN in Product Groups B, C, D, or E in Category 3 of the Commerce Control List that the individual or entity knows will be used in the development or production of ICs at any semiconductor fabrication facility located in China, but for which the individual or entity does not know whether such semiconductor fabrication facility fabricates certain ICs such as advanced logic, NAND, and DRAM ICs; or in the servicing of any such items; and
- **Prohibition Category 3**: Any item not subject to the EAR and meeting the parameters of ECCNs 3B090, 3D001 (for 3B090), or 3E001 (for 3B090) regardless of the end use or end user; or in the servicing of any such items. Notably, there is no accompanying knowledge qualifier associated with this prohibition.

BIS subsequently released limited guidance concerning the application of these new rules, including important clarifications such as the definition of "facility" and excluding certain administrative and clerical activities from the new licensing requirement. Additionally, to minimize supply chain disruptions, BIS issued a temporary general license to permit companies headquartered in the United States or in a subset of other countries to continue exporting certain ICs and associated software and technology for specified purposes to their affiliates and subsidiaries located in China through April 7, 2023. BIS is expected to review the need to impose this range of new export control restrictions on other sector supply chains, including those supporting quantum computing and certain kinds of biotechnology. Although White House National Security Advisor Jake Sullivan famously summarized the U.S. approach to protecting critical technologies as "small yard, high fence," as a practical matter, the complex global supply chains involved in producing the most advanced chips and quantum computers will necessitate multilateral coordination to erect any such barrier.

3. Multilateral Controls

In an effort to further restrict China's access to such critical technologies, the Biden administration has engaged in extensive diplomatic efforts to encourage closely allied countries to adopt similar controls on chip-making equipment. News reports of an agreement among the United States, the Netherlands, and Japan—countries that are homes to some of the world's most advanced semiconductor equipment manufacturers—suggest that such multilateral controls are imminent. While sweeping, the new export controls on China can only extend so far under U.S. law, and the Biden administration has made clear that multilateral coordination is necessary to counter Chinese technological advances in critical technological fields.

4. China-Related Entity List and Unverified List Designations

While new tools received much of the attention, in 2022 traditional export controls remained a core element of U.S. efforts to counter Beijing as a strategic competitor as the Biden administration again made frequent use of the longstanding Entity List and Unverified List to target China-based entities. As noted in our 2021 Year-End Sanctions and Export Controls Update, the expanding size, scope, and profile of the Entity List has

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

begun to rival OFAC's SDN List as a tool of first resort when U.S. policymakers seek to wield coercive authority, especially against significant economic actors in major economies. Indeed, in a break from past practice, in 2022 the Biden administration often looked first to BIS to effect its China policy rather than OFAC and its SDN List. Among the more than 60 Chinese entities added to the Entity List during 2022 were numerous organizations associated with advanced ICs and semiconductors such as ***Yangtze Memory Technologies*** ("Yangtze Memory") and ***Hefei Core Storage Electronic Limited***. Entities can be designated to the Entity List upon a determination by the End-User Review Committee ("ERC")—which is composed of representatives of the U.S. Departments of Commerce, State, Defense, Energy and, where appropriate, the Treasury—that the entities pose a significant risk of involvement in activities contrary to the national security or foreign policy interests of the United States. Much like being added to the SDN List, the level of evidence needed to be included on the Entity List is minimal and far less than the "beyond a reasonable doubt" standard that U.S. courts use when assessing guilt or innocence. Despite this, the impact of being included on the Entity List can be catastrophic. Through Entity List designations, BIS prohibits the export of specified U.S.-origin items to designated entities without BIS licensing. BIS will typically announce either a policy of denial or ad hoc evaluation of license requests. The practical impact of any Entity List designation varies in part on the scope of items BIS defines as subject to the new export licensing requirement, which could include all or only some items that are subject to the EAR. Those exporting to parties on the Entity List are also precluded from making use of any BIS license exceptions. However, because the Entity List prohibition applies only to exports of items that are "subject to the EAR," even U.S. persons are still free to provide many kinds of services and to otherwise continue dealing with those designated in transactions that occur wholly outside of the United States and without items subject to the EAR. The ERC has over the past several years steadily expanded the bases upon which companies and other organizations may be designated to the Entity List. In the case of the Chinese entities designated this year, reasons given included engaging in proliferation activities, providing support to Russia's military and/or defense industrial base, engaging in deceptive practices to supply restricted items to Iran's military, and attempting to acquire U.S.-origin items in support of prohibited military applications. Notably, in December 2022, 35 Chinese entities (plus one related entity in Japan) were designated to the Entity List for a variety of reasons, including among them, acquiring or attempting to acquire U.S.-origin items to support China's military modernization. Throughout the year, BIS also made extensive use of the Unverified List to motivate named entities to comply with end-use checks. A foreign person may be added to the Unverified List when BIS (or U.S. Government officials acting on BIS's behalf) cannot verify that foreign person's *bona fides* (i.e., legitimacy and reliability relating to the end use and end user of items subject to the EAR) in the context of a transaction involving items subject to the EAR. This situation may occur when BIS cannot satisfactorily complete an end-use check, such as a pre-license check or a post-shipment verification, for reasons outside of the U.S. Government's control. Any exports, reexports, or in-country transfers to parties named on the Unverified List require the use of an Unverified List statement, and Unverified List parties are not eligible for license exceptions under the EAR that would otherwise be available to those parties but-for their designation to the list. As discussed in greater detail in Section IV.A, below, BIS has implemented a new two-step process whereby companies that do not complete requested end-use checks within 60 days will be added to the Unverified List, and if those companies are added to the Unverified List due to the host country's interference, after a subsequent 60 days of the end-use check not being completed, the company on the Unverified List will be transferred to the Entity List. In conjunction with the announcement of this new policy on October 13, 2022, 31 Chinese entities were added to the Unverified List, including Yangtze Memory, which, as discussed above, was subsequently moved to the Entity List for presenting a risk of diversion of U.S.-origin items to Entity List parties. Cooperation with end-use checks was also rewarded, with dozens of Chinese entities being removed from the Unverified List throughout the year, including 26 entities on December 16, 2022, after BIS was able to verify their *bona fides*. Moving forward, we expect the U.S. Government to continue its use of both the Entity List and Unverified List to target additional China-based entities that it finds pose risks to U.S. national security and foreign policy interests. **D. Defense**

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

Department List of Chinese Military Companies The U.S. Department of Defense is required by Section 1260H of the National Defense Authorization Act for Fiscal Year 2021 to publish, and periodically update, a list of "Chinese military companies" operating directly or indirectly in the United States. On October 5, 2022, the Defense Department released its most recent update to the Section 1260H List, which identifies 13 additional PRC-based entities, including facial-recognition software developer ***CloudWalk Technology***, as having links to the Chinese military. Inclusion on the Section 1260H List triggers certain U.S. Government procurement-related restrictions on the listed entities and on contractors that may use certain of their products and services, and can serve as a precursor to designation to other restricted party lists maintained by the U.S. Government such as OFAC's Non-SDN Chinese Military-Industrial Complex Companies ("NS-CMIC") List (which restricts U.S. person investments in certain publicly traded securities) or the U.S. Department of Commerce's Military End User List (which restricts exports of certain U.S.-origin items). At the very least, companies named by the Defense Department appear to be on the U.S. Government's radar and may be at elevated risk of becoming subject to such trade restrictions in the future. Many of our clients also use inclusion on the Section 1260H List as a "red flag" for potential diversion to military end uses and end users. **E. Investment Screening** In conjunction with export controls, the Biden administration, acting through the Committee of Foreign Investment in the United States ("CFIUS" or the "Committee"), continued to closely scrutinize acquisitions of, and investments in, U.S. businesses by Chinese investors. CFIUS is reliant on its expanded powers provided under the Foreign Investment Risk Review Modernization Act of 2018, which we analyzed in an earlier client alert. As discussed more fully in Section V.A, below, CFIUS appears to be especially focused on identifying non-notified transactions involving Chinese acquirors (i.e., transactions that have already been completed and which were not brought to CFIUS's attention), including through use of the Committee's increased monitoring and enforcement capabilities. During calendar year 2021, the most recent period for which data is available, Chinese investors largely eschewed the CFIUS short-form declaration process, filing only one declaration with the Committee. China's 2021 numbers are also consistent with the period from 2019 to 2021, during which Chinese investors submitted 86 notices, but only 9 declarations. This apparent preference of Chinese investors to forego the short-form declaration in favor of the *prima facia* lengthier notice process may indicate a calculus that, amid U.S.-China geopolitical tensions, the likelihood of the Committee clearing a transaction involving a Chinese investor through the scaled-down declaration process is quite low. In addition to the Committee's purview over inbound investments, there is growing momentum to establish a new outbound investment screening mechanism to restrict U.S. investments abroad. As discussed in Section V.D, below, both the White House and the U.S. Congress have advanced proposals to establish such a regime. Although the scope and contours of an outbound screening mechanism remain uncertain, should one materialize it is highly likely that the Biden administration—whether or not it mentions Beijing by name—would begin by restricting U.S. investments in sectors of China's economy deemed critical to U.S. national security such as artificial intelligence and semiconductor manufacturing. **III. U.S. Sanctions A. Iran** Amid continuing advances in Iran's nuclear program, Washington and Tehran entered 2022 with limited prospects for a return to the Joint Comprehensive Plan of Action ("JCPOA"), the 2015 Iran nuclear agreement which the Trump administration renounced in 2018. As the year progressed, any hopes for a return to negotiations faded further as Iran shipped arms to Russia in support of the war in Ukraine and cracked down on street protests at home following the September 2022 death of Mahsa Amini at the hands of Iran's Morality Police. With a return to the JCPOA seemingly not on the table any time soon, OFAC accelerated the pace of new Iran-related sanctions designations during the second half of 2022, and issued an expanded general license designed to facilitate ordinary Iranians' ability to access the internet. In an effort to limit one of Tehran's key sources of revenue, OFAC in June, July, August, September, and November 2022 added dozens of parties to the SDN List for their involvement in the Iranian petroleum and petrochemicals trade. Underscoring the extent of the Biden administration's concerns about Iranian actors supplying unmanned aerial vehicles ("UAVs") to Russia for use in conducting attacks in Ukraine, including on civilian infrastructure, OFAC announced waves of UAV-related designations in September and November 2022, and again in January and

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

February 2023. The U.S. Government also warned that "OFAC is prepared to use its broad targeting authorities against non-U.S. persons that provide ammunition or other support to the Russian Federation's military-industrial complex," suggesting that additional designations related to shipments of Iranian UAVs to Russia may be on the horizon. After widespread street protests erupted in September 2022 following Mahsa Amini's death, the Biden administration announced nine rounds of sanctions targeting Iranian government officials and entities for their involvement in violence against peaceful demonstrators or restricting Iranians' internet access. Among those designated were Iran's Morality Police, as well as the country's prosecutor general and interior minister. More designations of leading members of Iran's security apparatus are likely in 2023. As part of its suppression of protests, the Iranian government cut off internet access to the vast majority of its citizens, presumably to limit discussion of the regime's brutal crackdown and to curtail access to organizing tools. In the wake of these restrictions by the Islamic Republic, the United States in September 2022 announced the issuance of Iran General License ("GL") D-?2, which expands the scope of permitted exports to Iran of certain software, hardware, and services incident to internet-based communications. As we described in an earlier client alert, GL D-?2 supersedes and replaces a years-old general license with the aim of expanding internet access for Iranians. As described by the U.S. Department of State, the expanded flow of information enabled by the license is designed to "counter the Iranian government's efforts to surveil and censor its citizens" and "make sure the Iranian people are not kept isolated." Whereas now-superseded GL D-?1 only permitted software "necessary to enable" internet communications, GL D-?2 permits the exportation of software that is "incident to" or "enables" internet communications. And unlike GL D-?1, there is no requirement that the internet-based communications are "personal," which was a sticking point and compliance burden for the private sector. Among the ways that GL D-?2 makes it easier for Iranians to get online, U.S. officials have noted that "most importantly [this] expands the access of cloud-based services," so that virtual private networks, or VPNs, and anti-surveillance tools can be delivered to Iranians via the cloud. As a practical matter, GL D-?2 opens the door for technology companies to export tools and technologies that are listed in or covered by the license, which have the potential to enable ordinary Iranians to more easily access information online and use the internet to communicate with others inside and outside the country. **B. Syria** Consistent with OFAC's longstanding commitment that sanctions should be reversible in response to changes in circumstances or a target's behavior, OFAC during 2022 modestly eased sanctions under two of its most restrictive programs targeting Syria and Venezuela. With respect to Syria, in May 2022, OFAC issued a general license authorizing U.S. persons to engage in transactions that are ordinarily incident and necessary to activities in 12 specified economic sectors in four regions of northeast and northwest Syria that are presently outside the control of the regime of Syria's President Bashar al-Assad. Sectors covered by the license include, among others, agriculture, telecommunications, power grid infrastructure, construction, manufacturing, and trade—all of which appear to be key to eventually building a sustainable postwar economy. This policy change aimed to mitigate growing economic instability and to undercut support for Islamic State of Iraq and Syria ("ISIS") militants. As described by the U.S. Department of State, economic instability makes non-regime held areas of Syria "vulnerable to exploitation by terrorist groups, especially ISIS." Easing sanctions on select industries in those regions is therefore intended to boost "commercial activity and investment" and, as a result, "reduce the likelihood of ISIS's resurgence by combatting the conditions that enable its recruitment efforts and its support networks." Importantly, Syria remains a comprehensively sanctioned jurisdiction. As such, U.S. persons are, except as authorized by OFAC and BIS, generally prohibited from engaging in transactions involving Syria or its government. Although Syria General License 22, by virtue of its limitation to particular industries and regions, represents at most an incremental easing of those restrictions, it also potentially hints at the direction of travel of U.S. policy. In particular, this authorization raises the possibility that OFAC may be amenable to further easing of sanctions on Syria in the future—for example, if the Assad regime were to lose control over additional territory or take meaningful steps toward a political settlement to end the country's decade-long civil war. **C. Venezuela** On November 26, 2022, the regime of Venezuela's President Nicolás Maduro resumed negotiations in Mexico City with the country's democratic

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

opposition, in a move cautiously welcomed by the Biden administration. As part of the renewed talks, the two sides signed a humanitarian agreement on education, health, food security, flood response, and electricity programs, and agreed to continue negotiations concerning presidential elections scheduled for 2024. Following the renewed negotiations and the humanitarian agreement, OFAC issued Venezuela General License 41, which represents the first substantial de-escalation in the U.S. pressure campaign on the Maduro regime since 2018, when the former Trump administration prohibited virtually all U.S. nexus dealings involving Venezuela's crucial oil sector. In particular, GL 41 authorizes certain transactions related to the operation and management by one named U.S. energy company of its joint ventures in Venezuela involving the state-owned oil company ***Petróleos de Venezuela, S.A.*** ("PdVSA"), including: the production and lifting of petroleum or petroleum products produced by its joint ventures; the importation into the United States of such petroleum or petroleum products, provided they are first sold to the U.S. company or its subsidiaries; and the purchase and importation into Venezuela of goods or inputs related to the above activities such as diluents. Highlighting OFAC's limited and incremental approach to Venezuela sanctions relief, GL 41 excludes from its authorization, among other things, sales of petroleum or petroleum products for exportation to any jurisdiction other than the United States, as well as certain payments to the Government of Venezuela. Following the issuance of GL 41 in late November 2022, new reports indicated that OFAC could soon grant a similar license to a second U.S.-based energy company with substantial claims against the Venezuelan state. In light of the Biden administration's apparent success at bringing the Maduro regime to the negotiating table, the United States may further ease sanctions on Venezuela in the coming year. However, any such policy changes are contingent on the outcome of the Mexico City talks between the Maduro regime and the country's fractious opposition, as well as on tangible steps by the Maduro regime toward holding free and fair elections and in making good on their commitments to ease the humanitarian situation in Venezuela. **D. Nicaragua** In 2018, OFAC launched a new Nicaragua sanctions program pursuant to Executive Order 13851 in response to President Daniel Ortega's attacks on democratic institutions and violent responses to civil protests. After remaining narrowly circumscribed during its early years—involving designations of a small number of government officials, as well as members and close associates of the ruling Ortega family—the Nicaragua sanctions program expanded considerably during 2022 as the Biden administration designated more economically consequential actors and laid the groundwork to potentially impose restrictions on broader segments of Nicaragua's economy. In January 2022, following sham elections in which the Ortega regime detained seven rival political candidates and dozens of pro-democracy activists, OFAC designated two telecommunications regulators for state censorship and misinformation, plus three military officials—including Nicaragua's minister of defense—for state acts of violence. The United States also responded to the elections by steadily expanding sanctions on the country's lucrative gold sector, which could be used to generate hard currency to sustain the Ortega regime's hold on power. The first action to target Nicaragua's gold sector occurred in January 2022 with the designation of a director of the state-owned mining company ***Empresa Nicaraguense de Minas*** ("ENIMINAS"). OFAC continued its sanctions against Nicaragua's gold sector in June 2022 by blacklisting ENIMINAS itself, alongside the head of the company's board of directors. Finally, in October 2022, the United States further increased sanctions pressure by designating the Nicaraguan mining authority, the General Directorate of Mines, which largely took over management of the country's mining operations from ENIMINAS following the company's June 2022 addition to the SDN List. Also in October 2022, President Biden signed Executive Order 14088, which expands the legal authorities underpinning the Nicaragua sanctions program in two significant ways. First, E.O. 14088 specifically identifies operating in the gold sector of Nicaragua's economy as a potential basis for designation to the SDN List. Following the model pioneered in the Venezuela program (and later employed in Russia and Belarus), that Executive Order also grants the Secretary of the Treasury broad discretion to expand U.S. sanctions to target any other sector of the Nicaraguan economy as the Secretary may determine. Second, E.O. 14088 authorizes possible restrictions on imports from, exports to, and new investments in Nicaragua. Those two grants of authority, together with the designations described above, appear to mark the evolution of the Nicaragua program

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

from one that was initially focused principally on political officials and Ortega regime insiders into a considerably broader program that could soon restrict dealings involving key sectors of Nicaragua's economy. If the Venezuela model is any guide, in coming months OFAC could use its new authorities to target additional industries in which Nicaraguan state-owned enterprises play a prominent role such as in the country's oil or financial services sectors. Should relations between the United States and Nicaragua continue to deteriorate, OFAC could also look to impose sanctions on additional government officials and regime insiders. **E. Afghanistan** In the wake of the Taliban's *de facto* takeover of Afghanistan in August 2021, the United States was faced with a sanctions conundrum. It needed to facilitate humanitarian flows into Afghanistan, but could not do so while empowering (or enriching) the Taliban and its allies the Haqqani Network, both of which have been long-designated for terrorism. Within days of the fall of Kabul, the United States froze Afghanistan's foreign reserves located in the United States to limit the Taliban's access to capital. Building on that announcement, President Biden on February 11, 2022 signed Executive Order 14064, which requires that any U.S.-based assets belonging to Da Afghanistan Bank, the country's central bank, be blocked and transferred to a consolidated account at the Federal Reserve Bank of New York. Pending a court decision, approximately half of the funds blocked pursuant to E.O. 14064 would be accessible by U.S. victims of terrorism and the remaining half—equal to approximately $3.5 billion—would be used to benefit the Afghan people. In coordination with international partners, including the Swiss government and Afghan economic experts, the Biden administration subsequently announced the creation of the Switzerland-based Afghan Fund to protect and make targeted disbursements of that $3.5 billion of Afghan sovereign assets. The Taliban, meanwhile, labeled the Afghan Fund an "illegal venture" and vowed to penalize entities that support its activities. Efforts by outside aid organizations to deliver humanitarian relief to Afghanistan have been complicated by the fact that much of the Afghan government is subject to two sets of U.S. sanctions. First, although Afghanistan is *not* subject to comprehensive U.S. sanctions, the Taliban have been designated since 2001 pursuant to Executive Order 13224, which restricts dealings involving certain named individuals, groups, and entities referred to as Specially Designated Global Terrorists. Second, various groups closely affiliated with the Taliban, though not the Taliban itself, are designated as Foreign Terrorist Organizations. The Haqqani Network, members of which now occupy key Afghan government posts, is one such organization. With the continuing challenges faced by humanitarian agencies and facing a risk of famine and potential state failure, on February 25, 2022, OFAC issued a general license authorizing certain transactions involving Afghanistan and the Afghan government, and published related guidance. That general license authorizes certain transactions involving Afghanistan or governing institutions in Afghanistan, provided that no funds are transferred to the Taliban, the Haqqani Network, or any of their majority-owned entities, other than in connection with common governmental functions such as payment of taxes and receipt of permits and licenses. As a practical matter, the license appears to be designed to provide nongovernmental organizations, and their financial institutions, additional comfort to engage in transactions involving the Afghan state. This general license was very broad, and in line with the Biden administration's commitment to calibrating sanctions as much as possible so that innocent citizens are not harmed. As discussed in Section III.H, below, OFAC essentially expanded this policy across almost all of its sanctions programs toward the end of 2022, issuing general licenses and guidance to emphasize that humanitarian, agricultural, medical, and pharmaceutical trade are not the target of U.S. sanctions. In April 2022, OFAC also published a fact sheet regarding the provision of humanitarian assistance to Afghanistan and support for the Afghan people. The fact sheet does not provide new guidance, but rather consolidates key authorizations and guidance for humanitarian and other assistance to Afghanistan. The fact sheet emphasizes that there are no OFAC-administered sanctions that prohibit exports, financial transfers, or activities in Afghanistan, provided that sanctioned parties are not involved. Additionally, the fact sheet details the various OFAC general licenses that authorize transactions involving the Taliban and the Haqqani Network. **F. Myanmar** As we suggested in our 2021 Year-End Sanctions and Export Controls Update, President Biden has continued to take a calibrated and incremental approach to exerting economic pressure on Myanmar (also called "Burma") with new waves of sanctions designations under Executive Order 14014, as the

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

situation in the country has failed to improve since a violent military coup overthrew Myanmar's elected civilian government in February 2021. In recognition of the one-year anniversary of the coup, on January 31, 2022, OFAC designated to the SDN List three officials serving in Myanmar's military-controlled government—the Union Attorney General, the Chief Justice of the Supreme Court, and the Chairman of the Anti-Corruption Commission—for their roles in the prosecution of Myanmar's former civilian leaders and pro-democracy activists. The sanctions designations ultimately did not deter these prosecutions as Aung San Suu Kyi, Myanmar's former State Counselor and Nobel Peace Prize laureate, was convicted and sentenced to 33 years in prison. Win Myint Hlain, Myanmar's former president, was convicted and sentenced to 148 years in prison. Four former leaders and activists were convicted and later executed in July 2022. Jailing and executing political opponents and activists has helped the Myanmar military (called the "Tatmadaw") maintain its hold over the country, and we expect the Biden administration to continue targeting the people and institutions responsible—as happened on January 31, 2023 when OFAC designated a further round of Myanmar government officials and entities to mark the coup's second anniversary. OFAC has also gradually strengthened sanctions against the Tatmadaw's support system, repeatedly targeting non-U.S. persons for providing the regime in Yangon financial support, arms, and/or military equipment. In January 2022, a Yangon-based services and logistics company was designated for allegedly paying $3 million a year to sanctioned ***Myanma Economic Holdings Public Company Limited*** ("MEHL") to lease a shipping port. According to OFAC, these commercial payments amounted to "material support" to a blocked party, one of the designation criteria under E.O. 14014. In January, March, October, and November 2022, OFAC added various individuals and companies to the SDN List for each playing a significant role in the supply of weapons, armaments, missiles, aircraft, and other defense equipment to the Tatmadaw. Most of these parties were designated pursuant to E.O. 14014 for "operating in the defense sector of the Burmese economy," a designation basis that OFAC has frequently relied upon—likely because of its broad scope and the fact that formal ties to a sanctioned party are not required. In a prior client alert, we discussed how E.O. 14014 affords OFAC considerable flexibility in its sanctions-targeting decisions, and we have seen that play out in practice since then. Although this past year's sanctions designations may not have featured the broad collateral consequences of the MEHL and ***Myanmar Economic Corporation*** designations announced in March 2021, which we discussed in detail in an additional client alert, they demonstrate the incremental approach that has been a hallmark of Biden-era sanctions on Myanmar. OFAC's recent designations are also consistent with the Burma Business Advisory published on January 26, 2022, which warned of the risks of dealing in Myanmar military equipment and real estate. The Burma Business Advisory, issued jointly by the U.S. Department of the Treasury and five other Executive branch agencies, remains a helpful guide to understanding the areas of Myanmar's economy on which OFAC appears to be focused and which may present elevated sanctions-related risks going forward. Additionally, we note that on March 21, 2022, the U.S. Department of State determined that the Tatmadaw committed genocide and crimes against humanity for their violence against the Rohingya, a religious minority group in Myanmar, in 2016 and 2017. That formal determination, which follows several years of factual and legal assessments by the U.S. Government, likely further diminishes the prospects for an easing of U.S. sanctions on the Tatmadaw or its enablers in the near term. **G. Crypto/Virtual Currencies** OFAC's designations to the SDN List in 2022 and numerous enforcement actions reveal a continued focus on the virtual currency industry, as well as important linkages between virtual currency enforcement and other agency priorities such as efforts to counter Russian sanctions evasion. These actions also suggest OFAC's willingness to take unprecedented action to stay ahead of illicit actors searching for ways to shield their funds behind the unique privacy and obfuscation that virtual currency services can provide. On April 5, 2022, OFAC added darknet market ***Hydra Market*** ("Hydra") and the virtual currency exchange ***Garantex*** to the SDN List. The designations of Hydra and Garantex came in the wake of Treasury guidance, including both an OFAC FAQ and a FinCEN alert published in March 2022, warning U.S. businesses of the risk that sanctioned Russian persons may attempt to evade U.S. sanctions through virtual currency transactions. Russia-based Hydra had become infamous as the world's largest darknet market,

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

facilitating cryptocurrency transactions for a range of illicit goods and services, from narcotics to money laundering services. The takedown of Hydra was coordinated across several U.S. Government agencies, as well as in concert with international partners. In parallel with OFAC's designation, the U.S. Department of Justice announced criminal charges against a Russian national for his alleged role in administering Hydra and the German Federal Criminal Police seized Hydra's servers in Germany, physically shutting down the operation. Garantex, a virtual currency exchange operated out of Moscow, was designated by OFAC for its role in over $100 million of transactions associated with illicit actors and darknet markets, including approximately $2.6 million from Hydra. Garantex's addition to the SDN List built off of OFAC's first-ever virtual currency exchange designations last year, described in our 2021 Year-End Sanctions and Export Controls Update, which similarly targeted Russia-based exchanges facilitating transactions involving illicit proceeds. 2022 brought its own firsts with OFAC's first-ever designation of a virtual currency mixer, ***Blender.io*** ("Blender") in May 2022. Virtual currency mixers, as the name suggests, operate by mixing funds deposited by many users together before transmitting the funds to their individual recipients, obfuscating the counterparties of the transactions. The financial privacy advantages motivating the creation of mixers make them attractive to illicit actors, a trend Treasury identified in its 2022 National Money Laundering Risk Assessment. According to OFAC, Blender was used to process over $20 million of the proceeds stolen in a March 2022 virtual currency heist carried out by the Lazarus Group, the Democratic People's Republic of Korea ("DPRK" or "North Korea") state-sponsored cyber hacking group. OFAC further tied Blender to money-laundering schemes by ransomware groups, an issue that continues to be an OFAC enforcement priority in the virtual currency space. The Blender designation in May 2022 set the stage for OFAC's second designation of a virtual currency mixer, ***Tornado Cash***. Originally designated on August 8, 2022 pursuant to Executive Order 13694 for malicious cyber activity, OFAC asserted that Tornado Cash had been used to launder more than $7 billion worth of virtual currency, including over $455 million stolen by the Lazarus Group. Although following in the footsteps of the Blender designation, the Tornado Cash blacklisting was novel in its own right. Unlike Blender's centralized model (i.e., a single company processing the transactions), Tornado Cash's decentralized, smart contract model is essentially operated by self-executing code running on public blockchains without the need for human intervention. Tornado Cash's August 2022 designation pursuant to E.O. 13694 triggered widespread confusion over the consequences of the action, and even spurred lawsuits against OFAC, claiming the Tornado Cash designation amounted to sanctions against technology which exceeded OFAC's authority and infringed on First Amendment rights. OFAC initially responded to this pushback by issuing a series of FAQs to clarify the scope of the designation, including, for example, that a U.S. person would not be prohibited from making Tornado Cash's open-source code available online to view. Then, on November 8, 2022, OFAC simultaneously delisted and re-designated Tornado Cash, this time adding Executive Order 13722 as a second basis for the designation based on Tornado Cash's material support of the Lazarus Group, considered part of the Government of the DPRK under the North Korea Sanctions Regulations. Still, critics argue that there is no "person" to sanction, as that term is defined in the relevant Executive Orders (as "an individual or entity"), despite OFAC's reasoning that Tornado Cash falls within the definition of "entity" as a "a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization." Even amidst the confusion, what remains clear is that OFAC is continuing to focus on the virtual currency industry as a key battleground in combatting cyber-related crime and other malicious behavior. Rather than solely targeting the individuals perpetrating hacks and ransomware attacks, OFAC continues to expand its sanctions designations to include services on which bad actors rely to launder illicit funds. As OFAC continues to link these designations to other enforcement priorities, such as its Russia and North Korea sanctions, the pace of new cyber-related designations and related enforcement actions seems unlikely to slow. **H. Other Sanctions Developments**

1. Hostages and Wrongfully Detained U.S. Nationals Sanctions

On July 19, 2022, President Biden issued Executive Order 14078, which creates a new

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

sanctions program focused on hostage-taking and wrongfully detained U.S. nationals. The Executive Order, which came amid substantial public attention to the plight of Americans detained in Russia such as former Marine Paul Whelan and basketball star Brittney Griner, suggests that the U.S. Government is prepared to use economic coercion to secure the release of such individuals—though no such designations have been announced to date. Issued pursuant to multiple statutes, including the Robert Levinson Hostage Recovery and Hostage-Taking Accountability Act, E.O. 14078 authorizes the Secretary of State to impose blocking sanctions on any foreign person that the Secretary determines has been involved in the hostage-taking of a U.S. national or the wrongful detention of a U.S. national abroad. As a practical matter, the Executive Order appears designed to, by brandishing the prospect of sanctions, increase U.S. leverage in negotiations with hostage-takers and deter hostage-taking in the first instance.

2. Humanitarian Trade Authorizations

On December 20, 2022, the United States became the first country to implement United Nations ("UN") Security Council Resolution 2664, which seeks to facilitate humanitarian aid by creating a "humanitarian carveout" across UN sanctions regimes. To implement that resolution, OFAC issued or amended numerous general licenses across several sanctions programs to ensure that humanitarian aid can be effectively delivered to vulnerable populations while simultaneously denying resources to sanctioned actors. These general licenses provide explicit authorization, now standard across all OFAC sanctions programs, for four broad categories of activities, including: (1) the official business of the U.S. Government; (2) the official business of certain international organizations such as the United Nations and the International Red Cross; (3) certain humanitarian transactions in support of nongovernmental organizations' activities; and (4) humanitarian trade in agricultural commodities, medicine, and medical devices. The Biden administration has repeatedly emphasized that it will seek to enforce U.S. sanctions while supporting the flow of legitimate humanitarian aid. OFAC has now addressed this challenge by permitting humanitarian assistance across multiple U.S. sanctions programs that did not previously provide for such authorizations. **IV. U.S. Export Controls A. Commerce Department**

1. Controls on Emerging and Foundational Technologies

As made evident through U.S. policy toward Russia and China, in 2022 export controls continued their rise as indispensable and central tools to further broader U.S. national security interests. A key part of this strategy involved controls on newly defined "emerging and foundational technologies." Section 1758 of the Export Control Reform Act of 2018 ("ECRA") requires BIS to establish export controls on "emerging and foundational technologies" essential to the national security of the United States. Under this authority, between 2018 and 2021, BIS imposed 38 new controls on "emerging" technologies by modifying an existing ECCN or creating a new ECCN. However, questions persisted around when and how BIS would begin to place controls on "foundational" technologies, as neither ECRA nor BIS regulations provided a precise definition of what would constitute an "emerging" versus "foundational" technology. Finally resolving this uncertainty, on May 23, 2022 BIS clarified that the agency will no longer "draw[] a distinction between 'emerging' or 'foundational' technologies" and will instead use the umbrella term "Section 1758 technologies" going forward. BIS acknowledged that drawing this fine distinction was proving to be inefficient and unrealistic—technology could be simultaneously "emerging" (in that it is new technology not in general use) and "foundational" (in that it constitutes an improvement on existing technology). And as Assistant Secretary for Export Administration Thea Kendler remarked, BIS is "responsive to national security threats" generally, regardless of the formal identification of technologies. Following this announcement, BIS imposed new controls in August 2022 and January 2023, covering the following eight Section 1758 technologies:

- Two substrates of ultra-wide bandgap semiconductors (Gallium Oxide (Ga2O3) and diamond), each added to 3C001.e and f, 3C005.a and b, and 3C006;

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

- Electronic Computer Aided Design software specially designed for the development of integrated circuits with any Gate-All-Around Field-Effect Transistor structure, added as new ECCN 3D006;
- Pressure gain combustion technology for the production and development of gas turbine engine components or systems, added to 9E003.a.2.e; and
- Four marine toxins (brevetoxin, gonyautoxin, nodularin, and palytoxin), each added to 1C351.d.4, d.9, d.13, and d.14.

Between September and October 2022, BIS sought public comments regarding additional Section 1758 controls on automated peptide synthesizers. In light of the revised approach of BIS to holistically control "emerging and foundational" technologies, we expect to see more Section 1758 controls this year.

2. Controls on Cybersecurity Items

Controls on cybersecurity items endured a decade-long history of multilateral negotiation and domestic rulemaking process. The Wassenaar Arrangement—the multilateral agreement that underlies much of the EAR—initially decided on new controls on cybersecurity items in 2013, and BIS proposed a rule implementing these controls in 2015. However, upon receiving public comments about the adverse impact that this rule may have on legitimate cybersecurity research and incident response activities, BIS returned to the Wassenaar Arrangement for renegotiation, which concluded in 2017. In 2021, BIS solicited comments on an interim final rule that would implement the renegotiated controls on cybersecurity items and create a new License Exception Authorized Cybersecurity Exports ("ACE"). The effective date of this rule was subsequently delayed to March 7, 2022, however, following public comments. On May 26, 2022, BIS amended these cybersecurity controls in response to those public comments. Among others, the amendments included a clearly defined list of "government end users" for purposes of the new License Exception ACE; a parallel end-user restriction in License Exception Encryption Commodities, Software, and Technology ("ENC") to avoid potential loopholes; and general clarifying revisions to help industry understand and comply with the new controls. The cybersecurity controls exemplify the importance of industry and public feedback in the export controls rulemaking process.

3. Entity List and Unverified List

As noted above, designations to the Entity List this year most prominently featured actors in Russia, Belarus, and China, but were certainly not limited to those jurisdictions. Beyond Russia, Belarus, and China, two key themes among this year's designations were (1) diversion activities and risks to Russia, China, Iran, and Syria (as demonstrated in designations on June 30, December 8, and December 19, 2022) and (2) involvement in unsafeguarded nuclear activities (as demonstrated in designations on February 14, June 30, and December 8, 2022). Notably, a new and highly aggressive criterion for designation was announced on October 13, 2022, indicating BIS's willingness to make expansive use of the Entity List. On the same day that BIS implemented expansive semiconductor controls targeting China, the agency announced that sustained lack of cooperation by a host government to schedule and facilitate the completion of end-use checks may lead to an entity's designation to the Entity List. Pursuant to this new guidance, BIS has since moved nine Russian entities from the Unverified List to the Entity List and is expected to pay closer attention to long-term designees on the Unverified List.

4. EAR Enforcement Policy

In conjunction with its fortieth anniversary, BIS's Office of Export Enforcement engaged in a number of policy updates designed to expand and strengthen its administrative enforcement authorities. On June 6, 2022, as part of its new Russia and Belarus controls, BIS amended its enforcement regulations to allow BIS charging letters to be made publicly available once issued—not after the case has been concluded. According to BIS, this rule

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

is intended "to inform interested parties of ongoing enforcement efforts in a more timely way and educate the exporting community, particularly with respect to recent amendments to the EAR that could result in new bases for enforcement action." The first public charging letter was issued against Russian oligarch Roman Abramovich on the same day as the regulatory change. To date, BIS has published five public charging letters, which are accessible on the agency's website. On June 30, 2022, BIS further updated its enforcement policy through a memorandum (the "EAR Enforcement Memo") published by Assistant Secretary for Export Enforcement Matthew Axelrod. Highlighting the increased threat from the unauthorized release of U.S. technology to China, Russia, Iran, and North Korea, Assistant Secretary Axelrod announced four enhancements to BIS's enforcement policy:

- **Imposition of Significantly Higher Penalties**: BIS will more "aggressively and uniformly" categorize appropriate cases as "egregious" and apply aggravating factors to escalate penalty amounts. Accordingly, we are likely to see increased penalty amounts for export violations.
- **Using Non-Monetary Resolutions for Less Serious Violations**: At the same time, BIS will increase the use of non-monetary settlement agreements, such as increased training and export compliance requirements, for pending cases in which violations are not egregious and have not resulted in serious national security harm.
- **Elimination of "No Admit / No Deny" Settlements**: BIS will no longer allow settlements in which parties could resolve allegations against them while neither admitting nor denying their conduct. Moving forward, in order to reach a settlement agreement with reduced penalty, the party must admit that the underlying conduct in fact occurred.
- **Dual-Track Processing of Voluntary Self-Disclosures**: BIS will now institute a 60-day "fast track" review for voluntary self-disclosures that involve only minor or technical infractions. In contrast, for voluntary self-disclosures that involve more serious violations, BIS will conduct a more in-depth review, with a field agent, an Office of Chief Counsel attorney, and as relevant, a Department of Justice attorney.

Except for the use of non-monetary resolutions, each of the enforcement policy changes suggests heightened risks of regulatory scrutiny, penalties, and reputational harm as a result of export violations. Assistant Secretary Axelrod also signaled that BIS may consider further changes "to maximize the effectiveness of [its] administrative enforcement of export violations." More than ever, it will be important for exporters to review the adequacy of their export compliance program and ensure compliance by their employees.

5. Antiboycott Enforcement Policy

Consistent with BIS's focus on enhanced enforcement of export regulations, BIS also enhanced its enforcement posture with respect to the antiboycott regulations. The antiboycott regulations prohibit compliance with foreign boycotts that are not sanctioned by the United States, with three categories of violations under Categories A, B, and C. On October 7, 2022, BIS adjusted these categories, with Category A now reflecting only those violations that are deemed the most serious and that will ordinarily warrant the maximum penalty available under the law, and Category B now reflecting violations that most commonly and currently arise in commercial transactions and subject to enhanced penalties to "promote awareness, accountability and deterrence." Together with the category adjustments, Assistant Secretary Axelrod published another memorandum providing updated antiboycott enforcement policies (the "Antiboycott Enforcement Memo"). Parallel to the EAR Enforcement Memo, the Antiboycott Enforcement Memo also indicated heightened enforcement priorities of BIS:

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

- **Enhanced Penalties**: BIS will impose higher penalties across the three categories of antiboycott violations.
- **Admissions of Misconduct**: BIS will require admissions of misconduct when settling matters involving antiboycott violations.
- **Renewed Focus on Foreign Subsidiaries of U.S. Companies**: BIS enforcement focus will be on foreign subsidiaries of U.S. companies involved in violations of U.S. antiboycott regulations.

In announcing these policy changes, Assistant Secretary Axelrod highlighted the "symbolic importance" of antiboycott rules in advancing U.S. foreign policy interests and preventing unlawful discrimination and committed to "vigorously enforce" the antiboycott rules. U.S. firms with potential unsanctioned foreign boycotts exposure should therefore consider implementing robust policies to ensure antiboycott compliance. **B. State Department**

1. Regulatory Updates

The U.S. Department of State's Directorate of Defense Trade Controls ("DDTC") likewise undertook significant regulatory initiatives this year, paving the way for even more rulemaking efforts in the year to come. On March 23, 2022, DDTC announced the start of a "multi-year multi-rule project" to comprehensively review and update the International Traffic in Arms Regulations ("ITAR") for the first time since 1993—dubbed the "ITAR Reorganization" effort. The project's first step was implemented through amendments to the ITAR, which went into effect on September 6, 2022. This first set of amendments was made to better organize the definitions and guidance for regulated parties, and did not change any substantive requirements under the ITAR. On July 20, 2022, DDTC launched a pilot program for an Open General License ("OGL") mechanism, pursuant to its authority under Section 126.9(b) of the ITAR. As an initial action, the agency issued two OGLs effective from August 1, 2022 to July 31, 2023. OGL No. 1 permits the *retransfer* of unclassified defense articles to pre-approved parties in Australia, Canada, or the United Kingdom. OGL No. 2 permits the *reexport* of unclassified defense articles to pre-approved parties in Australia, Canada, or the United Kingdom. The OGLs allow regulated parties to reliably benefit from pre-existing general licenses rather than seeking specific authorizations for each transaction, providing much needed flexibility for the regulated parties and U.S. allies that are covered by the OGLs. According to an FAQ issued by DDTC, more OGLs may be on the horizon depending on the experience of the current pilot program. To better assess the impact of the pilot program, the OGLs impose certain recordkeeping and information-sharing requirements. DDTC made other regulatory updates throughout the year, including issuing updated guidance regarding authorization requests for exports of defense services by U.S. persons abroad and the proposed exclusion from its controls of the taking of defense articles by armed forces on a deployment or training exercise or of the export of a foreign defense article that entered the United States and is exported without modification and pursuant to an authorization. DDTC continues to recalibrate its regulations, and U.S. persons engaging in activities involving defense articles or defense services should remain attentive to DDTC's planned additional rulemakings in 2023.

2. Compliance Program Guidelines

On December 5, 2022, DDTC issued long-awaited International Traffic in Arms Regulations Compliance Program Guidelines (the "ITAR Guidelines") that set out DDTC's expectations for an effective ITAR compliance program. The ITAR Guidelines revise DDTC's prior guidance and are now structured similarly to sanctions and export controls compliance program guidelines issued by other agencies, such as the Framework for OFAC Compliance Commitments and BIS's Export Compliance Guidelines. Like the expectations announced by those two agencies, an ITAR compliance program should be tailored to each organization's specific risk profile. Additionally, regulated parties are encouraged to incorporate the following critical elements into an effective ITAR

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

compliance program: (1) management commitment; (2) DDTC registration, jurisdiction and classification, authorizations, and other ITAR activities; (3) recordkeeping; (4) detecting, reporting, and disclosing violations; (5) ITAR training; (6) risk assessments; (7) audits and compliance monitoring; and (8) a written ITAR compliance manual. **V. Committee on Foreign Investment in the United States (CFIUS)** In addition to sanctions and export controls, the Committee on Foreign Investment in the United States—the interagency committee tasked with reviewing the national security risks associated with foreign investments in U.S. companies—remained active during 2022 as the Committee reviewed a record number of filings and continued to especially closely scrutinize China-related deals. Over the past year, CFIUS also grew more institutionally mature as the Committee for the first time ever received explicit guidance from the White House regarding which national security factors to consider when reviewing covered transactions, published its first-ever enforcement and penalty guidelines similar to those long employed by other U.S. national security agencies, and prepared to operate alongside a brand new *outbound* investment screening mechanism that is widely expected to be unveiled by the United States in coming months. **A. CFIUS Annual Report** On August 2, 2022, CFIUS published its annual report to Congress detailing the Committee's activity during calendar year 2021 (the "CFIUS Annual Report"). During that period, there was a record increase in CFIUS filings and the Committee indicated its continued focus on transactions that may pose national security risks. As noted in our prior client alert, our key takeaways from the CFIUS Annual Report include:

- CFIUS reviewed a record number of filings in 2021 (436 filings, up 39 percent from 2020), reflecting the strong mergers and acquisitions ("M&A") market in 2021. Of these filings, 164 (38 percent) were declarations and 272 (62 percent) were written notices. Parties were increasingly filing declarations voluntarily, given that less than one-third of the declarations filed in 2021 were subject to mandatory requirements.
- There was also a significant jump in withdrawn notices in 2021—from 29 in 2020 to 74 in 2021. While the parties filed a new notice following most of the withdrawn notices (85 percent of the total notices filed) in 2021, 11 notices (4 percent of the total notices filed) were withdrawn and the underlying transaction was not consummated either (1) due to CFIUS informing the parties that the Committee could not identify mitigation measures that would resolve national security concerns or the parties rejected CFIUS's proposed mitigation measures, or (2) for commercial reasons.
- 2021 was the first year since 2016 in which no Presidential decisions were issued blocking proposed transactions.
- Canadian investors accounted for the largest number of declarations in 2021 (13 percent of the total number of declarations filed). Australia, Germany, Japan, South Korea, Singapore, and the United Kingdom, traditionally seen by the U.S. Government as countries that present lower national security risks to the United States, accounted for approximately 38 percent of the total declarations submitted in 2021. Investors from Canada, Japan, and the United Kingdom submitted the most declarations from 2019 to 2021. In contrast, Chinese investors generally preferred submitting notices instead of short-form declarations, which may be a result of the ongoing geopolitical tensions between Washington and Beijing and the low likelihood that CFIUS would clear a transaction involving a Chinese acquiror through the short-form declaration process.
- In 2021, the number of critical technologies filings CFIUS reviewed increased by 51 percent from 2020, with countries seen as traditionally allied with the United States accounting for most such acquisitions.
- CFIUS shortened its turnaround times to respond to draft notices (from approximately 9 business days in 2020 to 6 in 2021) and to accept a formal written notice after submission (from, on average, 7.7 business days in 2020 to 6 in 2021).
- CFIUS may identify and initiate unilateral review of an already-completed

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

transaction, and may request the parties submit a filing after the fact—the result of such post-transaction reviews could range from requiring the parties to engage in certain operational and management changes to address the Committee's national security concerns, or even potentially be mandated to unwind the transaction. CFIUS identified more non-notified/?non-declared transactions in 2021 (135 in 2021 compared to 117 in 2020), which appears to indicate the Committee's increased interest in identifying non-notified/?non-declared transactions, as well as the Committee's expanded resources for monitoring and enforcement activities.

In light of the Executive Order issued by President Biden directing the Committee to consider additional national security factors when it reviews transactions, as well as the Committee's release of its new Enforcement and Penalty Guidelines (both of which are discussed below), we expect the trend of increased CFIUS filings and reviews to continue, notwithstanding the impact of global economic uncertainty on M&A activity. **B. National Security Factors** In order "to ensure that the foreign investment review process remains responsive to an evolving national security landscape and the nature of the investments that pose related risks to national security," in September 2022, President Biden issued the first Executive Order in the history of CFIUS to provide explicit guidance to the Committee in conducting national security reviews of covered transactions. Elaborating on existing factors that CFIUS is mandated by statute to consider, Executive Order 14083 directs CFIUS to consider five factors that closely parallel the U.S. Government's broader approach to protect U.S. technological competitiveness and U.S. persons' personal data, as well as decrease U.S. reliance on foreign supply chains involving critical technologies and mitigate the impact of cybersecurity attacks. E.O. 14083 directs the Committee to consider the following, as appropriate:

- The resilience of critical U.S. supply chains that may have national security implications, including those outside of the defense industrial base;
- U.S. technological leadership in areas affecting U.S. national security, including but not limited to microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy, and climate adaptation technologies;
- Aggregate industry investment trends that may have consequences for a given transaction's impact on U.S. national security;
- Cybersecurity risks that threaten to impair national security; and
- Risks to U.S. persons' sensitive data.

For an in-depth analysis of the policy rationale for, and the practical implications of, each of the five national security factors articulated in E.O. 14083, please see our September 2022 client alert. While E.O. 14083 is groundbreaking as the first-ever Executive Order providing guidance concerning the CFIUS review process, that measure principally builds upon existing policy trendlines. Indeed, it is no surprise that advanced technologies, cybersecurity risks, supply chains, and sensitive data remain at the forefront of U.S. national security considerations. That said, this Executive Order directs CFIUS's national security risk analysis in a way that, as a practical matter, will continue to expand the Committee's review authority. Given the breadth of the five factors elucidated in the Executive Order, combined with the Biden administration's goals of prioritizing U.S. competitiveness in certain critical technology sectors, we expect that the number of transactions reviewed by the Committee will continue to grow. Prior to engaging in any M&A activity or investments involving U.S. businesses operating within the sectors implicated by the factors outlined above, transaction parties should carefully assess the likelihood of CFIUS review and the potential need to file a notice or declaration. **C. Enforcement and Penalty Guidelines** Amid the U.S. Government's increasing scrutiny of transactions involving foreign investments in U.S. companies or operations that potentially impact national security, the Committee in October 2022 issued its first-ever CFIUS Enforcement and Penalty Guidelines (the "CFIUS Guidelines"). The CFIUS

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

Guidelines are non-binding and do not expressly create any new authorities for the Committee, nor do they appear to be connected to any reported increase in enforcement actions. However, the issuance of the CFIUS Guidelines may signal the Committee's intent to enhance enforcement efforts to address national security concerns. The CFIUS Guidelines also provide the Committee's first public statement regarding the non-exhaustive aggravating and mitigating factors that the Committee will consider when determining the appropriate response to an alleged violation of its regulations. Under the CFIUS Guidelines, (1) failure to submit a mandatory declaration or notice in a timely manner, (2) failure to comply with CFIUS mitigation requirements when such mitigation has been imposed, and (3) material misstatements, omissions, or false or materially incomplete certifications made at any point during the CFIUS process each constitute a violation that the Committee may consider to be subject to enforcement and penalty. CFIUS has the authority to issue civil penalties up to $250,000 per violation for material misstatements, omissions, or false certifications. Failure to comply with mandatory declaration requirements or violation of a material provision of a mitigation agreement may result in a civil penalty not to exceed the greater of $250,000 or the *value of the transaction*. However, the Committee may exercise discretion by weighing all aggravating and mitigating factors, such that not all violations will result in a penalty or remedy. Examples of such factors, which should be generally familiar to those who have assessed corporate enforcement factors published by other agencies such as the Justice Department, OFAC, and BIS, include the extent to which the conduct impaired U.S. national security, the frequency and duration of the conduct at issue, and the subject person's history and familiarity with CFIUS, amongst others. In the CFIUS Guidelines, the Committee formally encourages timely voluntary self-disclosure of potential violations and notes that it will take such disclosures into account when determining its enforcement response to an alleged violation. However, unlike other agencies, the Committee does not explicitly offer any specific incentives for such disclosure, such as a reduction in the proposed penalty amount, within the CFIUS Guidelines—potentially reducing the likelihood that transaction parties may at their own initiative bring apparent violations to the Committee's attention. For a more detailed analysis of the CFIUS Guidelines, please see our October 2022 client alert. **D. Outbound Investment Screening** While CFIUS review of *inbound* investments into the United States has been a feature of U.S. trade controls for decades, U.S. policymakers have lately weighed creating an unprecedented *outbound* investment screening mechanism to scrutinize how U.S. persons deploy capital abroad. Momentum for such a regime appears to be driven in part by concerns among U.S. officials at the prospect of U.S. investors financing or otherwise enabling efforts by strategic competitors such as China to develop critical technologies within their own borders. Although officials are continuing to debate how to tailor any such regime to avoid unduly restricting investments that present little risk to U.S. national security, developments over the past few months suggest that the United States may be on the cusp of standing up an entirely new outbound investment review mechanism. The fiscal year 2023 omnibus spending bill signed into law on December 29, 2022 allocated funding to various government agencies, including the U.S. Department of the Treasury. A joint explanatory statement accompanying the bill encourages Treasury "to address the national security threats emanating from outbound investments from the United States in certain sectors that are critical for U.S. national security." Significantly, Treasury has 60 days to "submit a report describing such a program," including the resources needed over the next three years to establish and implement such a program. Observers of this space were not surprised by this request. Many U.S. policymakers have been vocal about their view that existing national security regulations are insufficient to address concerns surrounding the transfer of capital to countries of concern, particularly China and Russia. Although a proposal that would have created an outbound investment screening regime, the National Critical Capabilities Defense Act ("NCCDA"), was removed from the CHIPS Act in the summer of 2022 and failed to gain traction in other legislation, Congressional efforts to establish such a regime remain ongoing. Indeed, there are few (if any) other policy proposals that will be debated in the newly-divided Congress that could likely receive similar levels of bipartisan support. In a September 2022 letter to President Biden, prominent members of Congress urged the White House to move forward with Executive action "to safeguard our national security and supply chain resiliency on outbound

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

investments to foreign adversaries." The letter expressed the intent to follow Executive action with legislation, and included a reminder that this was the template used to establish CFIUS. While we may see a reintroduction of the NCCDA, the potential for Executive action on this topic remains a distinct possibility. Continuing its efforts to forge multilateral policies on core trade issues, the European Commission has been working in parallel with the United States and has indicated that it is prepared to revise the European Union's foreign direct investment regulations. In October 2022, the European Commission published its Work Program 2023, which outlines key initiatives and priorities for the coming year. Among those key initiatives is "develop[ing] a strong set of strategic trade and investment controls to strengthen [EU] economic security, while also working to diversify value chains." The European Commission further indicated that it plans to "examine whether additional tools are necessary in respect of outbound strategic investments controls." Although the exact parameters of an outbound investment screening mechanism remain to be seen, there are numerous ways—including through legislation, an Executive Order, or an agency pilot program—that such a regime could potentially come into existence. Given unsuccessful prior attempts at passing legislation, establishing such a regime via Executive Order appears increasingly likely, pending further consultation by the United States with its European allies. Substantively, such an Executive Order could prioritize transactions involving sectors such as quantum computing, artificial intelligence, and semiconductors. Indeed, it is noteworthy that during 2022 the conversation increasingly shifted from *whether* there should be an outbound screening mechanism in the first instance to *how* such a mechanism should be designed to best achieve national security objectives while minimizing the regulatory burden on U.S. investors. As we discuss in a recent article, critics of potential outbound investment regimes urge the U.S. Government to ensure that any such mechanism is targeted and narrow, to ensure that any review of transactions does not overlap with other national security regimes or unduly stifle investment flows. The efficacy of any outbound investment regime will depend in significant part on the clarity of the policy objectives to be achieved by any outbound review, including clearly identifying what gaps in existing regimes the program hopes to address. **VI. European Union A. Trade Controls on China** The European Union's posturing vis-à-vis China continues to evolve in light of a number of factors, such as China's countermeasures to EU sanctions on human rights, the deliberate exertion of economic coercion against the bloc, and Beijing's ambivalent position in relation to the war in Ukraine. All meaningful momentum to sign the Comprehensive Agreement on Investment—a proposed ambitious EU-China deal aimed at dismantling barriers to foreign direct investments—appears to have been lost, and European players have increasingly voiced concerns about Beijing's global influence and the ways in which it is being exerted. While China continues to be seen as a systemic rival rather than an explicit threat and the overall stance is not one of direct confrontation, the European Union has been taking some crucial steps in anticipation of a more antagonistic future. For instance, a proposed regulation is making its way through the European Union's standard legislative process and, if implemented, it would grant the European Commission the power to retaliate against instances of economic coercion aimed at interfering with the European Union's sovereign choices, with countermeasures comprising a wide range of restrictions related to trade, investment, and funding. Economic coercion has been increasingly deployed by Beijing in the past five years as a way of pursuing strategic and geopolitical goals, and EU Member States have become a target. While the proposed legal text does not mention China explicitly, it was proposed in parallel to China applying discriminatory and coercive measures against exports from Lithuania and exports of EU products containing Lithuanian content, after Lithuania allowed Taiwan to open a *de facto* embassy on its territory. Another example of trade policy tools being used to promote the European Union's values and strategic objectives is the European Commission's proposal for a regulation banning products made with forced labor from the EU market. Once again, while the proposed text does not mention China by name, it was published in response to a European Parliament resolution calling for measures to address the situation in Xinjiang shortly after the Uyghur Forced Labor Prevention Act, discussed in Section II.A, above, was enacted by the United States. Unlike the UFLPA, the proposed regulation would not adopt a rebuttable presumption that all goods manufactured in specific regions of the world are made with forced labor, as

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

goods of all kinds will be within scope, and the burden of proof will remain on enforcing agencies within the European Union. The range of activities covered by the regulation, however, would be broader than the UFLPA, as products made with forced labor would not only be subject to an import ban, but would also face export restrictions once they are in the European Union and may be withdrawn from market if they inadvertently find their way to EU consumers. This is a key difference between the European Union's proposed regulation and the UFLPA, as the European Union will not allow the re-routing and further export of goods which have been deemed to have been produced with forced labor. Individual EU Member States have also been active in seeking to address forced labor concerns. On January 1, 2023, the German Supply Chain Act ("LkSG") came into force for companies with more than 3,000 employees in Germany and that have their central administration, headquarters, registered office, or a branch office in Germany. Accordingly, the LkSG is now effective for all DAX 40 companies and many other German and multinational companies. As mentioned in our 2021 Year-End German Law Update, relevant companies must implement dedicated due diligence procedures to safeguard human rights and the environment in their own operations, as well as in their direct supply chains. Companies are also required to take remedial actions in case a violation of human rights such as forced labor or a violation of environmental standards has occurred or is imminent (for their direct supply chain) or in case they obtain "substantiated knowledge" of such violation. While the LkSG has introduced obligations also relevant in the context of allegations of forced labor in Xinjiang, it does not go as far as the UFLPA or the draft EU regulation on prohibiting products made with forced labor on the EU market. It remains to be seen how the German Federal Service for Economic Affairs and Export Control ("BAFA"), which has already published related FAQs and guidance, will enforce the LkSG. Similarly, the European Union has been deploying its centralized regulatory powers to better protect the EU economy from exogenous shocks. This past year, the Commission intensified its focus on strengthening European resilience to supply chain disruptions and achieving strategic autonomy for semiconductors given the ongoing shortages in Europe and elsewhere. The proposed European CHIPS Act is deliberately designed to reduce dependence on non-allies, to focus collaboration efforts on countries like the United States and Japan, and to preserve the competitiveness of EU industries. In a similar vein, the European Union is enhancing its enforcement concerning distortive market practices with its new Foreign Subsidies Regulation, which is designed to even the playing field between EU businesses—which are under strict scrutiny whenever subsidized by EU Member State governments—and some of their heavily subsidized competitors such as Chinese state-backed companies. With these measures, the European Union is demonstrating that it is taking Chinese competition more seriously, and the further deployment of trade tools is expected as geopolitical events unfold. **B. Sanctions Developments**

1. Institutional and Procedural Developments within the European Union

While the European Union has been at the forefront in implementing sanctions against Russia with an impressive total of nine sanctions packages adopted in 2022, the Russia crisis has underscored some of the weaknesses in the European Union's sanctions and trade controls enforcement mechanisms and implementation procedures. The unanimity requirement for Common Foreign and Security Policy measures has led to perverse instances where a single Member State (such as Hungary with respect to the Russia oil import ban) can threaten to block the implementation of EU sanctions, and the lack of uniform enforcement among Member States has posed issues for cross-border operators. In particular, with sanctions being a foreign policy tool, the difficulty in aligning 27 potentially divergent national security interests has been a recurring theme of the past year. To begin addressing these shortcomings, the European Council adopted a decision adding sanctions violations to the "list of EU crimes" pursuant to Article 83 of the Treaty on the Functioning of the European Union and, shortly after, the European Commission followed with its proposal for a Directive containing minimum rules on the definition of the new criminal offenses covered and the applicable penalties. The Directive will have to be adopted by the Council and the European Parliament, yet these developments mark significant milestones in the European Union's increased efforts to harmonize EU sanctions enforcement, to close existing legal loopholes resulting from a fragmented

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

enforcement approach, and to ultimately increase the deterrent effect of violating EU sanctions. Furthermore, the European Parliament called on the Council to make use of provisions within the Treaty on European Union that would allow it to take certain decisions without military implications, in particular those concerning sanctions and human rights, by qualified majority rather than unanimity. This could break the logjam and the unsustainable reality in which one or two recalcitrant EU Member States could hold the will of the European Union hostage. This is essentially what occurred during the European Union's negotiations concerning the Russia crude oil import ban which saw Hungary as the sole holdout, delaying the bloc's finalizing of this measure. Discussions on qualified-majority voting are ongoing and are likely to be protracted given the delicate constitutional questions that such a move would raise, but the strengthening of the European Union's sanctions implementation and enforcement powers has gained a priority spot on the bloc's foreign policy agenda. Finally, to assist competent authorities in EU Member States with their enforcement efforts, the Commission launched the EU Sanctions Whistleblower Tool, which can be used for the anonymous reporting of past, ongoing, or planned sanctions violations, as well as attempts to circumvent EU sanctions regulations. More aggressive enforcement trends are expected in 2023.

2. Measures Targeting Russia's Supporters

The European Union has taken a more decisive stance towards those who assist Russia in its invasion of Ukraine, and its growing confidence in the use of sanctions as a foreign policy tool is evident in this context. In particular, the European Union has significantly expanded the list of Belarusians and Iranians subject to restrictive measures. Iran has developed and delivered UAVs to Russia for use against Ukraine, while Belarus has allowed Russia to fire ballistic missiles from its territory and enabled transportation of Russian military equipment. A number of Iranian individuals and entities have been sanctioned, including military commanders and UAV manufacturers. Meanwhile, Belarus has been hit with a gradually more severe range of sanctions, spanning from asset freezes on individuals and companies, sectoral financial sanctions, trade restrictions, removal of major banks from the SWIFT messaging system, a prohibition on transactions with the country's central bank, and others. In 2023, we can expect to see the European Union expand its use of sanctions tools to target Russia's supporters and further protect the bloc's security interests. Provision has been made within the EU Russia sanctions regime to designate those who actively facilitate infringements of the prohibition against circumvention. Although this criteria has not yet been used, it lays the groundwork to broaden the reach of EU sanctions without having to institute a new behavior-based or country-based regime. Separately, Iran has also been subject to additional restrictive measures due to domestic human rights violations.

3. Sanctions Enforcement in Germany

The past year also saw the development of German sanctions enforcement mechanisms. In May 2022, Germany enacted the Sanctions Enforcement Act I ("SDG I") containing short-term measures in order to enhance German sanctions enforcement. In particular, this Act now empowers authorities to summon and question witnesses, seize evidence, search homes and business premises, inspect registers, and preliminarily seize assets until clarification of ownership. Other measures introduced by the SDG I included a better exchange of sanctions-related information between authorities and additional competences of federal authorities such as the German Federal Financial Supervisory Authority ("BaFin") and the Central Office for Financial Transaction Investigations (the German Financial Intelligence Unit). In December 2022, Germany enacted the Sanctions Enforcement Act II ("SDG II"), which brought about structural improvements of sanctions enforcement in Germany. The SDG II created a new federal body—the Central Department for Sanctions Enforcement (which could become a German equivalent to the United Kingdom's Office of Financial Sanctions Implementation, discussed in Section VII.B, below). The Central Department has been given broad powers to identify and seize assets and to manage a sanctions violation whistleblower system. The Department also has the authority to appoint a monitor to supervise sanctions compliance in companies

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

that have violated, or are at risk of violating, sanctions. **C. Export Controls Developments** Given the historic economic interdependence between the European Union and Russia, the most noteworthy development in the field of EU export controls in the past year has been the unprecedented wave of new measures imposed against Russia. The European Union had never subjected such a broad range of goods, including consumer goods, to export controls and import bans as stringent as those imposed in relation to Russia. Bilateral trade in goods and services between the European Union and Russia appears set to decline in 2023, in light of the ever-broader restrictions the European Union is implementing with each new sanctions package. The European Union has now tested the feasibility of a wide-ranging export controls regime and global trends point in the direction of export controls being further weaponized to protect national security and strategic interests. **D. Foreign Direct Investment Developments** In April 2022, the European Commission published new guidance relating to foreign direct investment from Russia and Belarus, in light of the heightened national security risk that investments by Russian and Belarusian investors in strategic sectors of the economy may pose to the European Union. The guidance called upon EU Member States to have in place effective foreign direct investment ("FDI") screening mechanisms, to enhance cooperation between authorities responsible for FDI screenings and those responsible for sanctions enforcement, and to ensure full compliance with anti-money laundering requirements to prevent the misuse of the EU financial system. While EU Member States are still far from adopting an approach to FDI screening as aggressive as the United States or the United Kingdom, as discussed below, we expect this to be an area of significant focus going forward. In fact, as noted above, the European Commission in its Work Program 2023 indicated that it is prepared to revise the union's FDI screening regulation to strengthen its functioning and effectiveness, and also mentioned the need for outbound strategic investment controls to be assessed during the course of the year. **VII. United Kingdom A. Trade Controls on China** As its foreign policy stance towards China is evolving, the United Kingdom is starting to sharpen the tools in its trade arsenal. In May 2022, the United Kingdom added China to the list of embargoed destinations for military exports. Additionally, while initially the United Kingdom had simply been transposing the trade remedies measures that it inherited from the European Union into domestic law, in December 2022 the UK Trade Remedies Authority ("TRA") conducted its first independent investigation into the need for measures to counter unfair imports causing harm to the UK market. This review culminated in the introduction of new anti-dumping duties on the import of aluminum extrusions from China to the United Kingdom. The TRA is a novel addition to the United Kingdom's post-Brexit trade apparatus, and we expect that the agency will take an increasingly proactive approach as the United Kingdom takes full charge over the protection of its internal market and domestic producers build a relationship with the agency. Duty levels, however, remain in the low double digits in line with EU precedent, rather than following the U.S. approach under which duties can range up to several hundreds of times the invoiced value of the goods. Furthermore, the Imports of Products of Forced Labour from Xinjiang (Prohibition) Bill (the "Forced Labor Bill") was laid before Parliament in May 2022. The Forced Labor Bill represents the UK equivalent to the Uyghur Forced Labor Prevention Act and, like its U.S. counterpart, aims to prohibit the import of products made with forced labor in the Xinjiang region and will require companies importing products from Xinjiang to the United Kingdom to provide proof that their supply chain does not involve forced labor. However, the Forced Labor Bill did not complete its passage before the end of the parliamentary session and will need to be reintroduced. Nevertheless, the UK Government has recently reinforced its concerns about the situation in Xinjiang, stating that it intends to introduce financial penalties for businesses that do not comply with their transparency obligations under the Modern Slavery Act, while continuing to keep the possibility of introducing import bans under close review. In the meantime, the Home Office, HM Revenue & Customs ("HMRC"), and the National Crime Agency were jointly sued in October 2022 by the nonprofit ***Global Legal Action Network*** and international advocacy group ***World Uyghur Congress***. According to the lawsuit, UK government agencies failed to investigate whether cotton imports from Xinjiang ought to be treated as "criminal property" under the Proceeds of Crime Act 2002 (the "2002 Act"), having potentially been obtained via criminal means such as exploitation of forced labor, human rights violations and, allegedly, money laundering schemes. This

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

failure to investigate was alleged to be in contravention of the Foreign Prison-Made Goods Act 1897 (the "1897 Act"), which prohibits the importation into the United Kingdom of goods produced in foreign prisons. A further claim related to the UK Border Force unlawfully fettering its discretion to investigate breaches of the 1897 Act by operating on a reactive, rather than proactive, basis. On January 20, 2023, a High Court judge dismissed the lawsuit on the basis that the plaintiffs' evidence lacked the necessary specificity required by the 1897 Act and the 2002 Act to prosecute in relation to criminal offenses and civil powers and stated that an investigation would have little prospect of a successful conclusion without the (unlikely) cooperation of PRC authorities. We expect more activist litigation in the United Kingdom and across Europe to stimulate legislative action until such time as laws tackling the issue of forced labor are implemented. Companies are encouraged to preempt the incoming wave of increased supply chain scrutiny by starting to strengthen internal controls. The lack of a clear direction of travel on China policy is a product of the complex UK-China relationship, which has been further complicated by multiple recent leadership changes in the United Kingdom. In November 2022, Prime Minister Rishi Sunak declared the "golden era" in UK-China relations to be over, accusing China of competing for global influence using all of the levers of state power. Shortly afterward, however, the Prime Minister reinstated funding—previously withheld by his predecessor—to the Great Britain-China Centre, an independent body in charge of facilitating dialogue between the two countries. Echoing the Prime Minister's public statements, the House of Commons Foreign Affairs Committee published a report supporting the designation of China as a "threat," rather than as a "systemic competitor," in the next iteration of the Government's foreign policy mission statement, known as the Integrated Review of Security, Defense, Development, and Foreign Policy (the "Integrated Review"). The Committee also called for such a designation to be followed by calibrated and proportionate wider policy change, with a particular focus on domestic resilience and security. The UK Government is expected to finalize its update of the Integrated Review in the first quarter of 2023, and the type of trade measures deployed going forward will be determined accordingly. **B. Sanctions Developments** The United Kingdom's newfound freedom to shape its foreign policy only with reference to the country's own national security interests (rather than in concert with the European Union) marked a significant shift in sanctions policy in the United Kingdom. London has sought closer alignment with the United States, and a whole-of-government approach is increasingly being adopted to tackle geopolitical crises that may impact the United Kingdom's interests. In the field of sanctions, the United Kingdom is wielding its power as a global financial hub, having outsourced large parts of the implementation of sanctions measures to its financial services sector, which acts as gatekeeper of a large portion of global investment and trade. As a consequence, the UK Government is investing in its Office of Financial Sanctions Implementation ("OFSI"), its key sanctions enforcement agency, most notably by doubling its staff over the course of 2022. The move is clearly in anticipation of more serious enforcement efforts. Furthermore, following implementation of the Economic Crime (Transparency and Enforcement) Act 2022, OFSI will be able to—like OFAC, its sister agency in the United States—impose civil monetary penalties on a strict liability basis. Not knowing or having reasonable cause to suspect that conduct involves a sanctions breach is therefore no longer a viable defense in UK enforcement actions. In a further shift from previous practice, OFSI has also been granted the power to publicize details of financial sanctions breaches, including a summary of the case and the identity of the person having committed the breach, in line with U.S.-style enforcement actions. Regardless of the size of the penalties involved, which have traditionally been a fraction of penalties imposed by OFAC, this novelty in the UK system dramatically increases reputational costs for companies subject to enforcement. As part of the United Kingdom's effort to bolster OFSI's enforcement capabilities, a strategic partnership between OFSI and OFAC was announced this past year. The partnership's main goal will be information sharing, and the United Kingdom will now be able to leverage OFAC's and the broader U.S. Government's investigative powers to pursue its own enforcement actions. In addition, officials from both units plan to exchange best practices, pool expertise, and align their implementation of economic sanctions, which may lead to a further Americanization of the United Kingdom's enforcement practices. The establishment of the partnership marks an important milestone in OFSI's development and, together with the

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

developments mentioned above, sends a clear signal of an increasing aggressiveness in approach from OFSI. While these developments have not yet translated into particularly noteworthy enforcement activity as government investigations into potential sanctions violations can last years, OFSI's workload nevertheless materially increased in 2022, as industry demanded guidance to navigate the complexities of the newly implemented sanctions against Russia. As reported in the agency's annual review, OFSI considered 147 reports of suspected financial sanctions breaches, a slight increase compared to the previous year. Interestingly, a significant number of those reports involved referrals from international partners, further evidencing the greater international cooperation that allied countries are striving to achieve. **C. Export Controls Developments**

1. Enforcement Overview

Another example of the United Kingdom's emboldened enforcement intentions can be found in the field of export controls. In February 2022, HM Revenue & Customs, the UK enforcement body for breaches of export controls, issued its single largest settlement of £2.7 million in relation to the unlicensed exports of military goods. The size of the settlement is likely a result of a recent increase in HMRC's resources for export control enforcement, which had previously been subject to concerns of being underfunded and not commensurate with the scale and complexity of the task. We are likely to see an increase in effectiveness of investigations in 2023, with more, and higher, compound settlements issued as more resources are utilized by HMRC for enforcement purposes. Despite the substantial settlement size, and despite requests from the United Kingdom's Parliamentary Committee on Arms Export Controls, HMRC maintained its policy of not publishing the identity of the exporter and the export destination. Given the shift in OFSI's stance in relation to the publication of details relating to sanctions enforcement actions, it is possible that HMRC may soon begin to make more details of export control violations publicly available.

2. Amendments to Export Control Order 2008

On May 19, 2022, an amendment to the Export Control Order 2008 entered into force. The unlicensed export of dual-use goods, software, or technology not specified in Annex I to the Dual-Use Regulation is prohibited when destined for any military, paramilitary, or police forces, security services, or intelligence services in an embargoed destination, as well as to any person involved in the procurement, research, development, production, or use of controlled items at the direction of such forces. This new control applies only where the exporter is informed by the UK Secretary of State that the goods caught are, or may be intended, in their entirety or in part, for use by the abovementioned users. Notably, the amendment added China, the Hong Kong Special Administrative Region, and the Macau Special Administrative Region to the list of embargoed destinations. Stripping any export control-related distinction between Hong Kong, Macau, and China is in line with U.S. decisions on the same.

3. Suspension of Open General Export Licenses for Russia

In light of Russia's expanded invasion of Ukraine, the UK Export Control Joint Unit ("ECJU") suspended all extant export licenses for dual-use items to Russia, as well as the approval of new export licenses to Russia. Russia was also removed as a permitted destination from nine open general export licenses, including those for oil and gas exploration, chemicals, and cryptographic development. Exporters are now required to apply for standard individual export licenses ("SIELs") in order to export items to Russia. The ECJU has committed to deciding on 70 percent of SIELs applications within 20 working days, and 99 percent of applications within 60 working days, yet delays have been common over the course of the year given the sheer volume of requests. We expect to see a significant improvement in application processing times during 2023. **D. Foreign Direct Investment Developments** The most explicit expression of the United Kingdom's all-of-government approach to serve the country's national security interests is the range of investment control measures adopted thanks to the powers conferred on the UK

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

Secretary of State for Business, Energy, and Industrial Strategy ("BEIS") by the recently enacted National Security and Investment Act 2021 (the "NSI Act"). The NSI Act grants BEIS the power to scrutinize, and potentially interfere with, transactions in order to protect UK national security. Mandatory notification by industry players will be triggered where a transaction involves one of 17 "sensitive" sectors, including energy, quantum technologies, data infrastructure, artificial intelligence, cryptographic authentication, and defense, among others, which have been selected with the United Kingdom's strategic interests in mind. In general terms, the NSI Act is the UK version of the United States' CFIUS regime, and, like its U.S. counterpart, has principally focused on countering Chinese influence over strategically relevant sectors of the UK economy. Remarkably, during its first year of operation, BEIS blocked or unwound five transactions. Among those five transactions, four involved Chinese investors, while the last and most recent concerned the acquisition of a UK broadband firm by a subsidiary of a Russian-backed company. The fact that China is disproportionately the focus of the regime is also apparent from BEIS's conditional decisions—that is, the agency's final orders imposing conditions precedent to the completion of a transaction or some ongoing requirements post-acquisition. Four of the nine conditional decisions issued during 2022 involved investors linked to China. Most notably, NSI Act powers have recently been used to retroactively unwind transactions that had already completed. In November 2022, the UK Government ordered Dutch-headquartered and Chinese-owned ***Nexperia*** to reverse its acquisition of ***Newport Wafer Fab***, which owns the United Kingdom's largest semiconductor fabrication facility. The prospect of compound semiconductor activities at the Newport site being controlled by Chinese investors was deemed a national security concern due in part to the fab's proximity to an industrial cluster, as the cluster could potentially be compromised and thus prevented from participating in future projects relevant to UK national security in view of the risk of technological expertise and know-how exchanges in the region. While the UK NSI Act is the product of a reinvigorated intention to mitigate risks to UK national security presented by certain foreign investments, the Nexperia case is also an example of successful lobbying by the United States. The UK Government had initially determined that the acquisition would not pose a national security concern. However, the Republican-led congressional China Task Force urged President Biden to engage the UK Government to block the acquisition and, if unsuccessful, to employ all tools necessary to achieve the intended objective including reconsidering the United Kingdom's position on the CFIUS list of Excepted Foreign States and applying targeted export controls on Newport Wafer Fab. In particular, the China Task Force raised concerns regarding Nexperia's ownership, claiming that it is effectively a PRC state-owned enterprise as the company is owned by a Shanghai-listed firm allegedly backed by the Chinese Communist Party. The UK Government ultimately appears to have concurred in that assessment as it ordered Nexperia to divest its interest in the UK-based fabrication facility, citing the potential risk to national security. The United Kingdom is expected to continue using all tools to protect itself from influence attempts by non-allies and, in light of the transatlantic collaboration trends outlined above, further alignment on the deployment of CFIUS and the NSI Act regime appears likely.

* * *

In short, 2022 was an extraordinarily active year in the world of U.S., EU, and UK trade controls. As Russia's war in Ukraine grinds on and relations between the United States and China remain fraught, we expect further seismic shifts, including the introduction of new outbound investment screening regimes, to keep multinational enterprises occupied throughout the months ahead.

The following Gibson Dunn lawyers assisted in preparing this client update: Scott Toussaint, Irene Polieri, Chris Mullen, Judith Alison Lee, Adam M. Smith, Stephenie Gosnell Handler, Michelle Kirschner, Patrick Doris, Benno Schwarz, Katharina Humphrey, Attila Borsos, Lena Sandberg, Christopher Timura, David Wolber, Felicia Chen, Mason Gauch, Hayley Lawrence, Allison Lewis, Nikita Malevanny, Jacob McGee, Annie Motto, Sarah Pongrace, Nick Rawlinson*, Anna Searcey, Samantha Sewall, Audi Syarief, and Claire Yi.

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

GIBSON DUNN

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or the following members and leaders of the firm's International Trade practice group:

United States Judith Alison Lee – Co-Chair, International Trade Practice, Washington, D.C. (+1 202-887-3591, jalee@gibsondunn.com) Ronald Kirk – Co-Chair, International Trade Practice, Dallas (+1 214-698-3295, rkirk@gibsondunn.com) Adam M. Smith – Washington, D.C. (+1 202-887-3547, asmith@gibsondunn.com) Stephenie Gosnell Handler – Washington, D.C. (+1 202-955-8510, shandler@gibsondunn.com) David P. Burns – Washington, D.C. (+1 202-887-3786, dburns@gibsondunn.com) Nicola T. Hanna – Los Angeles (+1 213-229-7269, nhanna@gibsondunn.com) Marcellus A. McRae – Los Angeles (+1 213-229-7675, mmcrae@gibsondunn.com) Courtney M. Brown – Washington, D.C. (+1 202-955-8685, cmbrown@gibsondunn.com) Christopher T. Timura – Washington, D.C. (+1 202-887-3690, ctimura@gibsondunn.com) Annie Motto – Washington, D.C. (+1 212-351-3803, amotto@gibsondunn.com) Chris R. Mullen – Washington, D.C. (+1 202-955-8250, cmullen@gibsondunn.com) Sarah L. Pongrace – New York (+1 212-351-3972, spongrace@gibsondunn.com) Samantha Sewall – Washington, D.C. (+1 202-887-3509, ssewall@gibsondunn.com) Audi K. Syarief – Washington, D.C. (+1 202-955-8266, asyarief@gibsondunn.com) Scott R. Toussaint – Washington, D.C. (+1 202-887-3588, stoussaint@gibsondunn.com) Shuo (Josh) Zhang – Washington, D.C. (+1 202-955-8270, szhang@gibsondunn.com)

Asia Kelly Austin – Hong Kong (+852 2214 3788, kaustin@gibsondunn.com) David A. Wolber – Hong Kong (+852 2214 3764, dwolber@gibsondunn.com) Qi Yue – Hong Kong – (+852 2214 3731, qyue@gibsondunn.com) Fang Xue – Beijing (+86 10 6502 8687, fxue@gibsondunn.com)

Europe Attila Borsos – Brussels (+32 2 554 72 10, aborsos@gibsondunn.com) Susy Bullock – London (+44 (0) 20 7071 4283, sbullock@gibsondunn.com) Patrick Doris – London (+44 (0) 207 071 4276, pdoris@gibsondunn.com) Sacha Harber-Kelly – London (+44 (0) 20 7071 4205, sharber-kelly@gibsondunn.com) Michelle M. Kirschner – London (+44 (0) 20 7071 4212, mkirschner@gibsondunn.com) Penny Madden – London (+44 (0) 20 7071 4226, pmadden@gibsondunn.com) Irene Polieri – London (+44 (0) 20 7071 4199, ipolieri@gibsondunn.com) Benno Schwarz – Munich (+49 89 189 33 110, bschwarz@gibsondunn.com) Nikita Malevanny – Munich (+49 89 189 33 160, nmalevanny@gibsondunn.com) **Nick Rawlinson is a recent law graduate practicing in the firm's New York office and not yet admitted to practice law.* © 2023 Gibson, Dunn & Crutcher LLP Attorney Advertising: The enclosed materials have been prepared for general informational purposes only and are not intended as legal advice. Please note, prior results do not guarantee a similar outcome.

Related Capabilities

International Trade Advisory and Enforcement

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**