WILSON SONSINI

NATIONAL SECURITY REGULATIONS 2022 YEAR IN REVIEW

Over the last several years, parties interested in acquiring, investing in, licensing from, or collaborating with U.S. businesses—particularly those working with exciting and novel technologies—have been forced to grapple extensively with a wide range of regulations concerning national security, and 2022 has been no different. Between the Committee on Foreign Investment in the United States (CFIUS or the Committee), export controls, sanctions, anti-money laundering (AML), and government contracts rules, a new emphasis on U.S. national security regulation has touched companies across the board. Abroad, too, a number of new developments in these fields continue to show that national security is no longer a regulatory touchstone for the United States alone—a trend we expect to continue into 2023.

A year marked by geopolitical turmoil—the Russian invasion of Ukraine, strained tensions between the U.S. and China over Taiwan and Xinjiang, and an uncharacteristically frosty relationship between the U.S. and Saudi Arabia—brought a series of significant changes to these national security regulatory regimes. U.S. government agencies announced and implemented new rules across this broad regulatory landscape, and key U.S. regulators have continued to act decisively in response to the geopolitical challenges posed by China and Russia. Below we summarize some of the most significant developments in national security regulation in 2022 and discuss early expectations for 2023—in both cases, changes that will impact how technology companies, life sciences companies, and their partners and investors will interact for years to come.

CFIUS and Foreign Direct Investment (FDI) Review

Last year brought a number of new changes and foreshadowed others. Domestically, highlights included a presidential directive weighing upon the CFIUS review process and increased chatter regarding a proposed new U.S. outbound foreign investment regime. Abroad, the UK analog to CFIUS was fully implemented, and it has already wielded its authority to block a number of foreign investments. The global appetite for open investment seems to be getting increasingly sidelined by national security concerns, a trend that began in the mid-2010s and has accelerated in an era that has ended the *Pax Europaea* and set U.S.-China relations back to historic lows.

A New "Reverse CFIUS"?

This past summer, we reported on a renewed push in Congress for creating an outbound foreign investment review regime in the United States. While the specific bill, the National Critical Capabilities Defense Act of 2022, did not pass either chamber, the animus behind the legislation remains and could potentially resurface in a future bill in the 118th Congress.

Under the terms of the bill, an interagency body called the "Committee on National Critical Capabilities"—similar in composition and operation to CFIUS—would review investments, services, and support provided by U.S. persons benefitting countries and entities of "concern," with the primary foci being Russia and the People's Republic of China. Despite objection from business interests and the U.S. Chamber of Commerce over the potentially onerous bureaucratic oversight and compliance burdens associated with the proposed review process, National Security Advisor Jake Sullivan signaled that the Biden Administration would likely sign such an initiative if passed by Congress, and recent reports indicate that absent legislation the administration may create a "reverse CFIUS" process through executive action alone, something it has not shied away from doing in 2022 as seen in the next item.

The CFIUS Executive Order

While the year passed without significant legislative action on the U.S. foreign investment regime, an Executive Order (EO) issued in September 2022 demonstrated the continuing profile of CFIUS in the post-Foreign Investment Risk Review Modernization Act of 2018 environment. President Biden's EO, detailing the types of national security risks and factors that should guide CFIUS's reviews, did not seem to materially change any of the committee's practices, which already focus on most—if not all—of these considerations.

Nonetheless, the EO was clearly issued to accomplish *some* goal, and we wrote in September regarding our predictions of what may have motivated the EO, which included: resolving internal debates between relatively hawkish and dovish members of CFIUS, highlighting the U.S.'s continuing focus on China and Russia, or simply recognizing the increased prominence of CFIUS in the present day. Since September, we've seen the CFIUS enforcement team take a more pronounced interest in investment from nations that are not traditionally adversarial to the U.S., especially in sectors named in the EO. The apparent

goal of these enforcement requests—as anticipated in our EO mailer—appears to be to search for more attenuated potential connections to adversarial nations through outside investors—whether or not, e.g., Chinese contacts are immediately apparent.

Cracking Under Pressure?

Speaking of CFIUS's day-to-day, the Committee's 2021 annual report (released this past August) provided a mixed outlook for its operative efficiency. While CFIUS touted increased efficiency in its resolution of cases—including all-time high clearance rates in resolution of Declarations and initial Notice reviews—we noted that the same report also indicated that reviews are slowing down significantly for cases proceeding past the initial review period. A significant number of withdrawals and refilings were required in 2021 for these reasons, constituting nearly a quarter of all notices filed that year, and we expect a similar outcome for 2022, as scrutiny on Chinese and Russian investments (and investments with significant ties to China or Russia) at CFIUS has only intensified.

A Running Start for the UK National Security and Investment Act

Across the pond, the UK's National Security and Investment (NSI) Act entered into full force at the beginning of 2022. Despite the political turmoil that the UK experienced in the latter half of 2022, the Department for Business, Energy, and Industrial Strategy (BEIS) carried through a significant number of actions under the NSI Act.

Specifically, BEIS's power was brought to bear upon a number of transactions, beginning in July 2022 with blocking orders filed in a University of Manchester—Beijing Infinite intellectual property licensing arrangement; then the acquisition of electronic design automation firm Pulsic by Chinese chip-design software developer Super Orange HK acquisition; and most recently on the acquisition of Britain's largest chip-making fab, the Newport Waber Fab, by Chinese semiconductor manufacturer Nexperia.

These actions demonstrate that the UK government is not shying away from taking action even in the new regime's relative infancy. As BEIS continues to conduct additional reviews, call in additional investments, and impose additional final orders, we will continue to get a sense of how aggressively BEIS will assert its foreign investment review authority in the years to come.

Looking Ahead

Here in the U.S., the "reverse CFIUS" process mentioned above is expected to arrive via executive order sometime this year. Discussions within the administration and with outside stakeholders are ongoing, and the scope of the initial outbound screening regime continues to be difficult to predict as a result. However, a core emphasis on the development of selected key technologies—e.g., semiconductors—in China appears to be a very safe bet.

Overseas, meanwhile, in 2023 the Netherlands, Belgium, and Ireland are all expected to become the EU's newest member states to introduce new or improved FDI screening regimes, the latest in a gradual series of regimes implemented since the 2019 EU FDI Screening Regulation. These additions leave only a small handful of member states without such a screening regime, most of which—all except Bulgaria and Cyprus—have been making significant strides towards establishing their own regimes through legislative and regulatory processes. We expect that many of these such regimes will be announced, and potentially even activated, throughout 2023.

Export Controls

It's been a busy year for the export controls community. Beginning in February 2022 after Russia's invasion of Ukraine, we saw the rapid rollout of myriad export controls aimed at limiting the Russia's ability to continue its aggression, the Bureau of Industry and Security (BIS)'s issuance of new enforcement guidelines, and the Directorate of Defense Trade Controls (DDTC)'s International Traffic in Arms Regulations (ITAR) reorganization and new compliance guidelines.

Then, headlining the export controls news last fall was BIS's October release of long-anticipated controls on the export of advanced computing chips and semiconductor manufacturing equipment to China. The same day, BIS also announced a new end-use check policy, a move that escalated a long-running dispute between BIS and the Chinese Ministry of Commerce (MOFCOM).

New Export Controls "Put-in" Place to Restrain Russia

Following the Russian invasion of Ukraine, the U.S. government implemented multiple tranches of export controls aimed at depriving Russia (and neighboring ally Belarus) of products and material that could assist the Russian military campaign in Ukraine. Throughout 2022, these newly implemented export controls reached the following categories of exports:

- All items on the Commerce Control List (i.e., Export Administration Regulations (EAR) items that are not EAR99)
- Some EAR99 items, including
  - Schedule B Goods listed in Supp. 2 and Supp. 4 to Part 746 of the EAR, designating materials relevant to certain specific sectors
  - "Luxury Goods" listed in Supp. 5 to Part 746 of the EAR
  - Chemicals list in Supp. 6 to Part 746 of the EAR
- Exports for military- or intelligence-related end-use or end-users
- Foreign products made with U.S. software or technology that are captured by new Foreign Direct Product Rules (at Section 734.9(f) and Section 734.9(g)) of the EAR)

BIS also restricted the availability of most License Exceptions, including AVS (Aircraft, Vessels, and Spacecraft) and ENC (Encryption items). In March 2022, BIS took the unprecedented step of publishing a list of commercial and private aircraft that were flown into Russia in apparent violation of the EAR and thereby became subject to general prohibitions on any dealings (purchasing financing, servicing, etc.) with the listed aircraft. BIS has since updated the list more than a dozen times and subjected numerous Russian airlines to Temporary Denial Orders based on their EAR violations. BIS also reiterated in an August update that prohibitions *do* apply to Russian- and Belarussian-owned or -controlled aircraft manufactured outside the United States but exceeding the *de minimis* U.S.-origin content thresholds.

Lastly, the Entity List was also expanded in late September to add nearly 400 Russian and Belarussian entities and individuals. As is generally the case with parties named on the Entity List, a BIS license is required for any transaction involving EAR-controlled items and a listed party.

Together, these new controls levied a large impact upon the Russian economy and military, and—together with new sanctions discussed below—are at least partially responsible for inhibiting Russia's military operations in Ukraine in the latter half of the year.

New Guidelines from BIS and DDTC

A mix of substantive policy changes and clean-up clarifications were introduced in new guidelines released by BIS and DDTC last year.

On the BIS side, new guidelines released mid-year announced multiple policy changes for the agency's Office of Export Enforcement (OEE), signaling an intensified focus on punitive enforcement strategies. First, OEE communicated its intention to levy "significantly higher" penalties to disincentivize export control circumvention and to incentivize investments in corporate compliance programs. Second, OEE planned to increase its use of nonmonetary penalties as an intermediate form of resolution between warning/no-action letters and violations with monetary settlements. Third, OEE announced its intention to stop permitting "no admit, no deny" settlements, which it believes will lead to increased factual transparency that will improve enforcement observers' ability to learn from other entities' violations. Lastly, OEE announced an internal voluntary self-disclosure processing and staffing change to enable the agency to quickly resolve less serious infractions and quickly staff more serious ones.

From DDTC, a March 2022 interim final rule previewed a reorganization and consolidation effort to enhance the clarity of the ITAR, without announcing any substantive changes to the regulations. Later in the year, DDTC also released new compliance guidelines aimed at providing exporters with an overview of the defense trade controls regulations and sharing elements of an effective ITAR compliance program, akin to BIS's Export Compliance Guidelines.

A Bonafide Bonanza: BIS's Busy Day

At the end of August 2022, AMD and Nvidia both publicly reported receiving 'is informed' letters from BIS regarding certain advanced computing chips that each company produces. News of BIS taking this action generated an expectation that broader export controls on advanced semiconductors were likely forthcoming. On October 7, 2022, BIS released an interim final rule imposing such controls, some of which applied immediately and others coming into effect over the successive weeks.

Among other things (see our extensive write-up here), the interim final rule 1) imposed new export controls upon advanced chips, supercomputers, and semiconductor manufacturing equipment, 2) expanded the controls on foreign produced semiconductor and computing products, 3) created a prohibition on U.S. persons supporting the development or production of leading edge semiconductors in the People's Republic of China, and 4) implemented new end-use controls on supercomputers located in or destined for the People's Republic of China. FAQs from BIS relating to the new rules have been promised, but as of the time of drafting only limited guidance

has been issued. The same day, BIS *also* rolled out a new end-use check policy, escalating a tense stalemate with MOFCOM that endured for much of the pandemic, when COVID-19 restrictions were blamed for preventing BIS from conducting end-use checks for entities located in the People's Republic of China.

Under BIS's new policy, entities that failed to complete BIS's requested verifications would be placed on the Unverified List, and 60 days later would be nominated for inclusion on the Entity List, regardless of whether the importer or their government was the proximate cause of BIS's inability to complete its verifications. Alongside the announcement, BIS immediately added 30 entities to the Unverified List (including prominent flash memory manufacturer Yangtze Memory Technologies Co.), which started the clock for further escalation should BIS's end-use checks continue to be obstructed. At the same time, BIS removed a small handful of companies from the Unverified List—and removed more later in the fall—presumably because those companies had completed the required end-use checks with the support of MOFCOM.

Export Controls Forecast

With the semiconductor rules released and with the semiconductor industry wrangling with new economic challenges as the pandemic-era shortages morph into a modern-day glut, we expect that the Biden Administration may turn to consider new controls for other emerging fields and technologies in the back half of the term, whether within or outside of the Wassenaar Arrangement.

While the U.S. continues to pursue unilateral controls with increased frequency—as it did in the semiconductor context last year—other countries are reportedly on the precipice of joining. Despite earlier indications that the Netherlands and Japan did not plan to follow the U.S. plan to significantly restrict exports of semiconductors and semiconductor manufacturing equipment, recent reports indicate that both countries have now agreed to join in principle.

Foremost among industries considered for export controls is quantum computing, which has created a recurring wedge between security hawks clamoring to prevent Chinese development in the sector and private sector players who fear that export controls could "torpedo" the U.S.'s own development (and commercial leadership) in the relatively nascent field. Although the latter argument has generally carried the day even into 2022, given the frequency of reported discussions between the Department of Commerce and industry players, we would not be surprised to see new controls added as quantum continues to advance in the coming years.

Beyond quantum computing, National Security Advisor Jake Sullivan has hinted that the Biden Administration may also be considering new export controls on technology in artificial intelligence, biotechnologies, and clean energy, while also dramatically expanding the use case for export controls to promote human rights, democracy, and privacy goals. Should those goals be implemented in practice, we may see many more "BIS Bonanzas" in 2023.

Going forward, the export controls rolled out for Russia in 2022 could be applied to other contexts as well. Should the geopolitical situation worsen elsewhere in the world—especially in the Asia-Pacific region—we anticipate that these export controls could have an especially severe and wide-reaching impact on U.S. businesses due to the relatively deep interconnectedness between the U.S. and key Asian economies.

Sanctions

If China was the primary target of this past fall's export controls updates, Russia was equally (if not more so) the intended target of 2022's sanctions actions. Beyond the significant changes to controls on exports to Russia and Belarus described above, we recount some of the most significant sanctions news of the year below.

"A Round" and "a Round" and "a Round" We Go

Both in the run-up to and following Russia's invasion of Ukraine back in February 2022, Western countries implemented a series of sanctions packages in response. Throughout the year, as the war dragged on, successive rounds of sanctions followed. All in all, the EU, UK, U.S., Canada, and other allied nations collectively implemented dozens of rounds of sanctions on Russian entities and key Russian politicians, businessmen, and government figures.

In late February, immediately prior to the invasion, the Biden Administration expanded the territorial reach of comprehensive sanctions that were already in place in Russia-occupied Crimea to include two additional separatist-controlled territories of Ukraine, the Donetsk People's Republic, and the Luhansk People's Republic regions. These comprehensive sanctions prohibit new investment in these

regions; the import into the United States of goods, services, or technology from these regions; the export from the United States of goods, services, or technology to these regions; and the facilitation of any such transactions by U.S. persons.

With the military invasion of Ukraine days later, additional sanctions (and export controls followed), with new OFAC directives severely curtailing activities involving large Russian enterprises (such as Sberbank and Gazprom) and dozens of Russian and Belarussian entities being added to the Specially Designated Nationals and Blocked Persons list.

In the months since, further additions to sanctions lists have become routine, usually announced in conjunction with the EU and other G7 countries—such as numerous prohibitions covering new investment and the provision of legal advisory, architectural, engineering, and IT consultancy services—with no sign of them stopping in 2023. Following these sanctions, government officials in the U.S., UK, and EU have signaled an uptick of sanctions enforcement activity, as the focus of the government's sanctions program transitions from establishment to execution, a trend that will likely continue as the conflict nears its anniversary.

AML

In the AML world, 2022 was a year marked by the use of traditional enforcement tools in nontraditional settings and against nontraditional financial institutions. Without novel legislative authority, FinCEN worked to apply existing rules and regulations against an economy increasingly using crypto- and virtual currencies.

With deeper legislative and regulatory changes still on the horizon, 2023 may prove an even busier time at the U.S. Department of the Treasury despite crypto investors themselves retrenching significantly compared to this time a year ago.

Executive Order on Ensuring Responsible Development of Digital Assets

Back in March 2022, when Bitcoin prices hovered around $40,000, the White House released a new EO establishing a digital assets policy strategy for the federal government. This regulatory framework pushed forward broad, overarching tenets of the U.S. government's relationship with digital currencies, built around principles like financial stability, consumer protection, economic leadership, and responsible innovation. More specific policies—such as the U.S. Securities and Exchange Commission's treatment of digital assets—remained unresolved. But while prices of digital assets trended downward as the year carried on, policymaking interest seemed to stay at or near record highs throughout 2022.

Alphabet Soup: AML, MSBs, KYC, and NFTs

Amidst the frenzy of "speculative madness" that non-fungible tokens (NFTs) experienced in the beginning of the year, we put together some helpful guidelines to help companies mitigate AML risks when entering (or dabbling in) the NFT market, as did the Treasury in a report, *Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art*. Though the value proposition of the NFT market may have shifted over the course of the year, our guidance remains on point—and enforcement actions taken last year by FinCEN against money-services businesses (MSBs) like Tornado and Blender.io demonstrate the costs associated with failing to meet the sometimes-demanding compliance requirements (often including robust Know-Your-Customer (KYC) programs) associated with operating in this area.

AML in the Metaverse

While we contend that most employees at FinCEN couldn't give you a cogent description of the metaverse—a buzzword with no consensus on its definition yet— assuredly yes, AML laws apply there as well. Exactly what laws apply and what compliance actions are required depends on the real-world characterization of one's business and whether one is deemed to be an MSB. But as the world continues to digitalize and money laundering risks continue to exist and even escalate, "escaping to the metaverse" won't be a viable compliance program.

Update on the Beneficial Ownership Information Reporting Rule

While the brunt of the news regarding the beneficial ownership information (BOI) reporting rule was released alongside proposed regulations back in December 2021 (a subject analyzed in our first client advisory of 2022), the final rule was published in the Federal Register on September 30, 2022. The new BOI rule will come into effect on January 1, 2024, after which time millions of existing legal entities will be required to file information with FinCEN to disclose their beneficial owners or potentially be subject to civil and criminal penalties. In the meantime, enjoy your 2023—and consider checking some of our recent "Focus on Fintech" publications (here and here) if reading more is among your New Year's Resolutions.

Government Contracting

Finally, on the government contracting front, 2022 saw changes to both carrots and sticks in the regulatory regime. Early in the summer, the U.S. Department of Defense (DoD) tightened up cybersecurity requirements for contractors. Months later, windfall of CHIPS ("Creating Helpful Incentives to Produce Semiconductors") and Science Act subsidies for semiconductor companies came alongside a number of conditions, limitations, and resulting risks for businesses—and may portend a new era of U.S. industrial policy, much as the EU and Japan have been subsidizing technology development efforts in the past few years. Of course, such funding comes (and likely will continue to come) with the usual government contracting strings attached.

DoD Drums Up Demands on Data and Cyber

A midyear memorandum from DoD demonstrated that heightened interest in cybersecurity continues to proliferate across federal and state government agencies. The interagency memorandum, directed at DoD contracting officers, solely served to highlight the Defense Federal Acquisition Regulation Supplement (DFARS) requirement that contractors maintain "covered contractor information systems" protected by National Institute of Standards and Technology-compliant measures. In the event of breach, contract officers are instructed to seek remedies such as payment withholding, options cancellation, and partial or full contract termination.

With Great Subsidies Come Great Responsibility

The passage of the CHIPS and Science Act put $52 billion of government funding in play for companies, agencies, and public/private research institutions operating in or around the semiconductor industry. Scheduled to be allocated over the next five years, this funding was designed to ameliorate short-term chip shortages that constrained manufacturing in 2021 and early 2022 and to lay the groundwork for the United States to regain (and maintain) technological independence and leadership in the years ahead.

Alongside nearly $39 billion allocated to funding projects for constructing, expanding, and modernizing semiconductor manufacturing facilities and equipment, our write-up noted numerous conditions attached to the acceptance of these subsidies, including specific enumerated bidding requirements (from both the CHIPS Act and the National Defense Authorization Act), funding claw-back mechanisms, and covenants not to aid Chinese semiconductor manufacturing efforts. In addition, numerous levels of oversight will likely accompany the distribution of funds under this program, which the Department of Commerce has already begun building up in earnest.

Moreover, the CHIPS Act was only one of several initiatives that signal the U.S. recommitment to industrial policy. In the energy sector, for example, new laws such as the Inflation Reduction Act of 2022 and the Bipartisan Infrastructure Law combined with the CHIPS Act to offer hundreds of billions of dollars for clean energy investment. Attorneys in Wilson Sonsini's energy and climate solutions practice are continuing to track those federal funding opportunities here.

Conclusion

After another blockbuster year for CFIUS, FDI, sanctions, export controls, and other related practice areas, there do not appear to be any signs of a slowdown in the national security sector. As the Biden administration continues to tweak U.S. foreign policy to contain Russia, China, and other geopolitical competitors, Wilson Sonsini's national security practice will be sure to keep you abreast of the latest developments.

In the meantime, please feel free to contact Josephine Aiello LeBeau (jalebeau@wsgr.com), Stephen Heifetz (sheifetz@wsgr.com), Joshua Gruenspecht (jgruenspecht@wsgr.com), Mike Casey (mcasey@wsgr.com), Anne Seymour (aseymour@wsgr.com), Seth Cowell (scowell@wsgr.com), Jahna Hartwig (jhartwig@wsgr.com), or any member of the national security practice at Wilson Sonsini Goodrich & Rosati with any questions or additional information about the developments noted in this *National Security Regulations 2022 Year in Review*.

WILSON SONSINI

650 Page Mill Road, Palo Alto, California 94304-1050 | Phone 650-493-9300 | Fax 650-493-6811 | www.wsgr.com

Wilson Sonsini has 19 offices in technology and business hubs worldwide. For more information, visit wsgr.com/offices.