WILSON SONSINI

NATIONAL SECURITY REGULATIONS 2020 YEAR IN REVIEW

In the last several years, parties interacting with U.S. businesses—particularly U.S. businesses with novel technologies—have grappled with a wide range of national security regulations. From the Committee on Foreign Investment in the United States (CFIUS) to export controls, sanctions to anti-money laundering, or telecommunications national security regulations to government contracts rules, a new emphasis on U.S. national security regulation has reached companies across the board.

This past year brought a series of particularly 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 announced or signaled a new proactive approach to enforcement of rules touching on a variety of national security concerns. Parties involved in the U.S. telecommunications sector even saw the creation of a new (yet familiar) telecommunications regulator. Below we summarize some of the most significant developments in national security regulation from 2020—changes that will impact how technology companies and their partners and investors will interact for years to come.

CFIUS

The year 2020 marked an inflection point for CFIUS, which conducts national security reviews of foreign investments in, and acquisitions of, U.S. businesses. Since the 2018 enactment of CFIUS reform legislation—the Foreign Investment Risk Review Modernization Act (FIRRMA)—CFIUS has been proceeding at a breakneck pace to implement its new FIRRMA powers, an implementation process that is now largely complete.

CFIUS Finalizes Its Rules Under FIRRMA

FIRRMA broadened CFIUS's jurisdiction, created categories of transactions for which CFIUS filings are mandatory, and infused CFIUS with increased resources. In January 2020, the U.S. Department of the Treasury, acting as CFIUS chair, released final rules (effective on February 13, 2020) that replaced a 15-month "pilot program." These rules permanently gave CFIUS expanded jurisdiction over "TID U.S. businesses" and created two types of mandatory filings for certain transactions involving these TID U.S. businesses.

More specifically, combining the new rules and old rules that have been maintained, the following broadened range of investments are now subject to CFIUS jurisdiction:

- Those in which a foreign person—broadly defined such that even a U.S. fund may be a foreign person if certain foreign indicia are present—will obtain "control" over any U.S. business, where control may be found if there is more than a 10 percent voting stake, a board seat, or significant veto authority; and
- Those in which a foreign person will make an investment in, and obtain either control or a non-controlling "triggering right" in, a "TID U.S. business."
  - Triggering rights are the following:
    - a board seat or observer seat, or nomination rights; or
    - access to material non-public technical information; or
    - involvement in company decision-making.
  - A TID U.S. business is a business involved with:
    - Critical **T**echnologies
    - Critical **I**nfrastructure
    - Sensitive Personal **D**ata.

CFIUS's authority to review a transaction, as outlined above, is very broad and now extends beyond "control" investments to investments of even less than 1 percent (if the U.S. business is a TID business and the foreign investor obtains triggering rights). Currently, however, filings with CFIUS are *mandatory* only for i) certain transactions with a TID U.S. business involved with "critical technologies" and ii) when a foreign government-backed investor obtains a "substantial interest" in a TID U.S. business. If a filing is not mandatory but the transaction is subject to CFIUS's jurisdiction, the parties can make a voluntary filing to obtain a safe harbor against adverse CFIUS action. Alternatively, the parties can refrain from making a filing and take the risk of adverse CFIUS action, which exists in perpetuity but may be low or high, depending on the nature of the transaction (see information below on the enforcement regime).

Following the February implementation of the bulk of the new FIRRMA rules, in May 2020 CFIUS implemented filing fees, scaled to the value of the transaction (with no fee triggered for transactions of $500,000 or less and the highest fee of $300,000 applying to transactions of $750 million or more). The fees generally apply to long-form "notice" filings but not to short-form "declarations." A variety of considerations, apart from the fees, inform whether parties should choose to file a notice or a declaration.

Finally, on October 15, 2020, CFIUS implemented a tweak to the mandatory filing rules for investments in companies with "critical technologies." Specifically,

this change replaced an old piece of the mandatory filing test that required parties to discern whether critical technologies were being designed for or used in designated "sensitive industries." The new test asks instead whether a U.S. regulatory authorization (e.g., an export control license) is required for the export or transfer of such technologies to the investing entity or certain affiliated parties (particularly stakeholders of 25 percent or more in an investing entity).

The Enforcement Regime Takes Shape

While finalizing the new rules, CFIUS also turned its attention to enforcement. Leveraging resources mandated by FIRRMA, CFIUS created a dedicated enforcement unit and launched an enforcement website, including an email tipline. Equipped with the new enforcement team, CFIUS throughout 2020 escalated its outreach to parties that had not made filings to CFIUS.

While in 2018-2019 the private sector focused heavily on the creation of the FIRRMA mandatory filing rules, this new 2020 enforcement initiative by CFIUS frequently concerned transactions subject to CFIUS's broader elective jurisdiction.

Indeed, while we are not yet aware of CFIUS having levied any enforcement penalties against parties for failure to make a mandatory filing, we are aware of CFIUS reaching out in numerous cases inquiring about CFIUS jurisdiction with respect to transactions within their elective jurisdiction, and compelling filings in some of these cases. In addition, CFIUS informally has indicated that it expects to levy penalties for failing to make mandatory filings in appropriate cases going forward. Furthermore, the universe of transactions upon which CFIUS could levy such penalties is likely to expand based on the email tipline, which could ratchet up enforcement activity by giving commercial competitors a mechanism to create CFIUS troubles for their rivals.

Ultimately, CFIUS's enhanced enforcement is likely to change the calculus for investors who otherwise may be disinclined to make a filing. This is likeliest to come into play for venture investments or acquisitions involving more sensitive investors—including Chinese or Russian acquirers—and/or more sensitive industries, such as semiconductors, advanced battery technologies, and gene-sequencing technologies.

Taken as a whole, the new CFIUS rules and enforcement regime have already had far-reaching implications for businesses in a wide array of sectors and for investors of almost all foreign nationalities that invest in those businesses—including indirect investments made via many U.S. private equity and venture funds. As CFIUS rounds into form in 2021 and begins flexing its newfound enforcement powers, the reach of the committee may well continue to expand.

Export Controls

The year 2020 was momentous for the U.S. export control system, particularly with respect to the Export Administration Regulations (EAR) administered by the Department of Commerce, Bureau of Industry and Security (BIS). Noteworthy events included, as noted above, a tying of export classifications directly to CFIUS mandatory filing requirements, the designation and control of certain "emerging technologies," a vast expansion of the extraterritorial reach of the U.S. export licensing requirements, and heightened reporting and licensing requirements relating to Russia, China, and Venezuela.

CFIUS Critical Technology Analysis and Designation of Emerging Technologies

As discussed above, CFIUS regulations implemented in February 2020 include mandatory filing requirements for certain investments in companies involved with "critical technologies." A "critical technology" is any technology, software, or commodity covered by any one of several U.S. government lists, including the EAR's Commerce Control List (CCL). Thus, whether a CFIUS filing is mandatory now depends on the U.S. business's export control classifications, even when the U.S. business does not export anything. The importance of export classifications was heightened in October 2020, when CFIUS amended its regulations to tie the critical technology mandatory filing requirement to the question of whether a U.S. business's critical technology requires a license or other authorization.

Thus, knowing the export classification control numbers (ECCNs) and the related export licensing requirements is now essential for CFIUS compliance as well as U.S. export controls compliance. Significant penalties can be imposed under both regimes for non-compliance.

Additionally, in 2020, BIS began to implement a technology designation mandate of the Export Control Reform Act (ECRA), which was companion legislation enacted with FIRRMA in 2018 (the latter CFIUS reform legislation discussed in the CFIUS developments section above). The ECRA called for the designation of "emerging" and "foundational" technologies, as subsets

of "critical technologies." Accordingly, in 2020 BIS implemented new controls on 37 emerging technologies.

The industries most likely affected by the new controls are aerospace, biotechnology, chemical, electronics, encryption, geospatial imagery, and marine. The designated emerging technologies include: hybrid additive manufacturing/computer numerically controlled tools, specific computational lithography software, certain technology for finishing wafers for 5nm production, limited digital forensic tools, certain software for monitoring communications from a telecommunications service, sub-orbital aircraft, 24 chemical weapons precursors, discrete microwave transistors, continuity of operation software, post-quantum cryptography, underwater transducers designed to operate as hydrophones, air-launch platforms, and geospatial AI imagery software.

Expansion of Extraterritorial Reach and Increased Licensing Requirements Relating to Huawei

Since May 2019, BIS has added Huawei Technologies Co., Ltd. (Huawei) and more than 100 of its affiliates (collectively "Huawei entities") to BIS's Entity List (explained below); BIS made these additions because of a belief that these companies were acting contrary to U.S. national security and foreign policy interests.

These Entity List designations are significant because any item (technology, commodity, or software) subject to the EAR now requires a BIS license if Huawei entities are involved in the transaction. In August 2020, BIS significantly expanded the concept of "items subject to the EAR" for foreign-produced items and, thus, the licensing requirements for the Huawei entities. More specifically, in August, BIS expanded the EAR's jurisdiction to include transactions involving foreign-produced and foreign-developed items that have minimal nexus to the U.S.—the minimal nexus to the U.S. will suffice when a Huawei entity is involved. The expanded jurisdiction covers foreign-produced items, including foreign-produced commercial off-the-shelf items, developed or produced from specified U.S. technology and software (or SUST/S), including being produced in a plant using SUST/S, when a Huawei entity is a party to the transaction.

Consequently, a foreign item designed using U.S.-origin electronic design software classified under ECCN 3D991 or another SUST/S for end-use in a Huawei device now requires a BIS license. Further, a foreign designed and developed item that is simply tested on a U.S.-origin piece of test equipment classified under ECCN 3B991 or other SUST/S that is for incorporation into a Huawei device, even by a third party, requires a BIS license. It is important to note that these are merely illustrative examples of the extraterritorial reach under the August 2020 EAR amendment; they are not exhaustive.

Increasing License and Reporting Requirements on China, Russia, and Venezuela

In April 2020, BIS tightened controls on exports, reexports, and transfers in-country to China, Russia, Venezuela, and 20 additional countries; and BIS increased reporting requirements for exports to China, Russia, and Venezuela. These heightened export controls are designed to minimize the risk of diversion, particularly with respect to the use of technology, commodities, or software subject to U.S. export controls to benefit the military capabilities of China, Russia, and Venezuela.

To ensure compliance with these expanded U.S. controls, any U.S. business doing business with parties in China, Russia, or Venezuela should verify that they have export policies and procedures in place that include both classification and licensing procedures and robust Know Your Customer (KYC) measures.

Economic and Trade Sanctions Developments

The year 2020 will likely be remembered for the impact COVID-19 had worldwide, and the pandemic underlies several of the key trade-related national security developments this year. In addition, the strained relations between the U.S. and China led to the issuance of a number of sanctions-like actions against Chinese or China-related parties by executive order.

COVID-Related Considerations

In recognition of the need for humanitarian assistance, including for sanctioned countries, in April 2020, the Department of the Treasury's Office of Foreign Assets Control (OFAC) issued a fact sheet that summarized authorizations available for providing humanitarian assistance to combat COVID-19. The document consolidated guidance on the most relevant exemptions, exceptions, and authorizations under its sanctions programs related to Iran, Venezuela, North Korea, Syria, Cuba, and Ukraine/Russia. Specifically, OFAC provided a list of authorizations applicable to the provision of food, medicine, and

medical devices and emphasized its favorable licensing policy for items not covered by these authorizations that are needed to combat COVID-19. For instance, in October 2020, OFAC issued General License M to allow certain U.S.-based academic institutions to provide online educational services and related software to students located in Iran who were unable to return to the United States due to COVID-19.

U.S. Government Use of Sanctions As a Key Foreign Policy Tool

Throughout 2020, the administration continued to use OFAC sanctions and the threat of being added to OFAC's list of Specially Designated Nationals (SDN list) to express its displeasure and apply pressure to its adversaries. In June 2020, the administration issued an Executive Order authorizing sanctions against foreign persons who engaged in efforts by the International Criminal Court to investigate, arrest, detain, or prosecute U.S. or any U.S. ally personnel without the consent of the United States or that ally. The United States added a large number of persons and entities to the SDN list, including companies seen as associated with the Chinese, Venezuelan, or Cuban military, high-level government officials in these countries, and persons and entities in the petroleum sector, among other designations.

U.S.-China Trade Relations

In 2020, the pandemic only exacerbated the already strained trade relations between the United States and China. A broad range of U.S. government agencies imposed significant restrictions on doing business both with China as a whole and with key Chinese actors including Huawei Technologies Co., Ltd. (discussed in part in the export controls section above) and ByteDance/TikTok/WeChat. The United States continued its trend of using trade and economic sanctions to apply pressure by adding current and former senior officials of the Chinese Communist Party to the SDN list and by making additions in response to China's human rights abuses both in Hong Kong and against the Uyghur minority, as well as China's efforts to undermine democratic processes and threaten the autonomy of Hong Kong, and various U.S. government agencies composed lists of companies thought to have military or government connections. In November 2020, citing the International Emergency Economic Powers Act (IEEPA), President Trump issued an executive order that limited transactions involving publicly traded securities of selected companies designated on a Department of Defense list of Communist Chinese Military Companies, and left open the possibility of further similar sanctions. As of December 3, 2020, 35 companies, including Semiconductor Manufacturing International Corporation (SMIC), have been added to this list.

OFAC Cracks Down on Cyber and Other Crimes

OFAC also paid significant attention in 2020 to cybercrimes. Again, using the SDN list as a tool, OFAC added to the SDN list individuals and entities in Iran, North Korea, Russia, and other countries, because of their involvement in various cybercrimes. OFAC also expanded the list of digital currency addresses provided on the SDN list.

Further, in October 2020, OFAC published an advisory on the potential sanctions risks related to facilitating ransomware payments. In this advisory, OFAC discouraged ransomware payments based on its view that these payments would encourage future ransomware payment demands and could be used to fund activities adverse to the national security and foreign policy objectives of the United States. OFAC reminded individuals and institutions that these payments could violate OFAC regulations, encouraged proactive measures to protect against ransomware, and clarified that OFAC intended to find regulatory violations in cases where ransomware payments involved an SDN, blocked person, or a comprehensively embargoed jurisdiction. OFAC also issued an advisory in October clarifying that the "Berman Amendment" to the IEEPA, which generally exempts informational materials (including artwork) from regulation, does not exempt *all* dealings in artwork from OFAC regulation and enforcement. Specifically, OFAC stated that, in relation to high-value artwork, its regulations prohibit transactions involving artwork and a blocked person or SDN to the extent that the artwork functions primarily as an investment asset or medium of exchange.

Anti-Money Laundering

The year 2020 continued a trend, likely accelerated by the pandemic, of financial activity migrating online and often away from large financial institutions. As evidenced by the developments highlighted below, federal anti-money laundering (AML) regulators, including the Treasury Department's Financial Crimes Enforcement Network (FinCEN), are accordingly broadening their regulatory focus.

Enforcement of MSB Registration Requirements

On October 19, 2020, FinCEN assessed a $60 million civil money penalty against Larry Dean Harmon for his virtual currency anonymizing

services "Helix" and "Coin Ninja." The penalty, for willful violations of regulations applicable to money services businesses (MSBs), is a reminder of the importance of being attentive to MSB regulations, which FinCEN administers pursuant to the Bank Secrecy Act (BSA). The category of MSBs covers many subcategories of non-traditional financial institutions, such as money transmitters (broadly defined to cover those engaged in transmitting funds) and providers and sellers of prepaid access (which can include gift cards, in-game currency, and more). These subcategories cover an increasingly large amount of online activity, especially activity by fintech, e-commerce, and gaming companies.

FinCEN alleged that Harmon's cryptocurrency businesses failed to comply with three core requirements applicable to MSBs: i) failure to register the companies, ii) failure to maintain an AML program, and iii) failure to submit suspicious activity reports.

MSBs are required to register with FinCEN within 180 days after the business is established—regardless of whether the company is aware that it is an MSB. Harmon was found to have been operating Helix and Coin Ninja as unregistered MSBs, more specifically as "money transmitters." FinCEN may assess a civil penalty of $5,000 for each day an MSB operates while unregistered. As evidenced by the large penalty against Harmon, in this case, FinCEN found more than mere unintentional failure to comply with applicable registration requirements.

FinCEN Ransomware Guidance

FinCEN also published ransomware guidance (issued in conjunction with similar OFAC guidance discussed above) warning that payments to ransomware perpetrators—e.g., to unfreeze a computer system frozen by the ransomware perpetrator—might inadvertently make the payer a money transmitter.

FinCEN noted that ransomware has created a new market for those seeking protection against ransomware attacks. These protection services can include facilitating ransomware payments. However, a company making these payments might become a "money transmitter" and therefore be subject to regulation as an MSB. Any of these companies would be required to, among other things, register with FinCEN, maintain an AML program, and file suspicious activity reports. In extreme cases, a payer may have exposure to criminal liability and imprisonment, particularly under the criminal money laundering statutes at 18 U.S.C. §§ 1956, 1957, and 1960. This exposure is in addition to potential civil liability under FinCEN regulations and potential civil and criminal liability under OFAC regulations and related statutes.

FinCEN Proposes to Expand Its Travel and Recordkeeping Rules and Relax Its AML Program Rule

FinCEN also has taken recent action to update its regulations to address threats related to cross-border transactions. On October 27, 2020, FinCEN issued a proposed rule that would amend the so-called "Travel Rule" and related "Recordkeeping Rule," which collectively require financial institutions (including MSBs) to store information in connection with certain funds transfers and to send information with those transfers. The proposed rule would reduce certain thresholds as to when these rules apply and clarify that convertible virtual currency (including transfers of digital assets serving as legal tender) are covered by these rules.

In particular, under the proposed rule, financial institutions (including MSBs) would face a reduced threshold for requirements to collect, retain, and transmit certain information for cross-border transfers that begin or end in the United States. The current threshold is generally $3,000 (applicable to transfers regardless of whether those transfers are cross-border or not); the proposed rule would lower that threshold to $250 with respect to cross-border transfers that begin or end in the United States. This may result in a materially increased compliance burden for MSBs, particularly money transmitters. The opportunity for public comment on the proposed rule closed on November 27, 2020. FinCEN may issue a final rule at any time.

Additionally, in September 2020, FinCEN issued an advance notice of proposed rulemaking—a form of a "heads up" regarding a forthcoming proposed rule—that sought public comment on how the long-standing requirement to implement an AML program could be made more flexible and tailored to each institution's risk profile. Currently all financial institutions, including MSBs, are required to implement an AML program. The opportunity for public comment closed on November 16, 2020, but the public likely will have further opportunity to comment if and when FinCEN issues a proposed rule.

Telecommunications and National Security

The year 2020 also saw the debut of a new regulatory entity in the national security and technology space—albeit

one that had operated for decades on an informal basis: the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Team Telecom, or simply the Committee) whose primary objective is to assist the Federal Communications Commission (FCC) in its "public interest" review of license acquisitions or transfers with potential national security implications.

Goodbye, Team Telecom, and Hello... CAFPUSTSS?

The first significant event of 2020 was the presidential directive to formalize the Committee on April 4, 2020 pursuant to Executive Order (EO) 13913, which for the first time established an official process and timeline for the Committee's review of FCC license applications and transfers. Upon formation, the Committee stepped into the role previously performed by an unofficial body informally known as Team Telecom, which historically comprised the U.S. Department of Justice (DOJ), advised and informed by the Federal Bureau of Investigation, the U.S. Department of Defense (DOD), and, since its creation in 2004, the U.S. Department of Homeland Security.

EO 13913 identified the Committee's members as the Attorney General (who acts as the chair of the Committee), the Secretary of Defense and the Secretary of Homeland Security—effectively formalizing the Team Telecom composition. The Committee reviews all initial applications referred by the FCC, and the FCC appears to be continuing its practice of referring all applications that involve foreign participation. The Committee has 120 days to complete an initial review—which the Committee can extend another 90 days for a more thorough "additional assessment." Committee review will ultimately result in one of three outcomes: i) granting the application because it raises no national security risk; ii) addressing any national security risk by imposing mitigation measures; or iii) recommending that the FCC deny the application. EO 13913 also for the first time suggested that the Committee consider initiating reviews of existing foreign licenses by petitioning the FCC on point.

The FCC Buys into the New Team Telecom Rules

On September 30, 2020, the FCC incorporated many of the procedures set forth in EO 13913 into formal FCC rules in a Report and Order (the FCC Order). Unlike earlier iterations of Team Telecom, the Committee now has a formal role recognized in FCC regulations requiring its participation in a number of specific proceedings before the Commission. These include, but are not limited to, international section 214 applications (i.e., applications to provide telecommunications services across borders), submarine cable applications, and section 310(b) petitions (i.e., applications to exceed the FCC's default foreign ownership limitations across a number of different services, including broadcast and wireless spectrum ownership).

In addition, for the first time, the FCC Order requires parties to submit the types of information that the Committee uses to assess national security risk as part of the original application to the FCC itself. The International Bureau at the FCC is charged with creating a set of standard questions for submission with all FCC applications, covering a range of areas of potential national security interest. The Committee may follow up with more tailored questions after it reviews those responses, but must do so on a relatively rapid timescale. Given the historical delays associated with the Team Telecom process, the EO and FCC Order hold out hope of expediting this particularly opaque national security review.

With the publication of the FCC Order in the Federal Register on November 27, 2020, the new era for Team Telecom will kick off right before the new year, on December 28, 2020. However, the changes to the FCC rules for interactions with the Committee will continue into 2021, with the publication of the standard questions and beyond.

Who Is on the Radar?

Early returns on reviews of license applications in 2020 signaled the new Committee's direction and priorities. Just a few days after EO 13913 was issued, on April 9, 2020, the DOJ announced that it had recommended that the FCC revoke and terminate China Telecom Corp., Ltd. 2007 Section 214 authorization to provide international telecommunications services to and from the United States. The DOJ, along with other participating Executive Branch agencies, cited "substantial and unacceptable national security and law enforcement risks" associated with China Telecom's operations, along with China Telecom's failure to comply with aspects of a prior Letter of Assurance it signed with the FCC, as making the FCC's prior authorizations to China Telecom inconsistent with the public interest. Soon thereafter, on June 17, 2020, Team Telecom followed up with a recommendation that that the FCC deny Pacific Light Cable Network System's Hong Kong undersea cable connection to the United States. These

recommendations follow the FCC's May 2019 denial of a license request from China Mobile Ltd, effectively barring the company from operating in the United States, which at the time was the first public block of a license application at the recommendation of Team Telecom.

Taken together, these events send a clear signal that the U.S. government is preparing a more muscular and aggressive telecommunications regulatory regime to protect U.S. national security that, while facially neutral, in practice appears to be oriented toward a specific perceived geopolitical adversary in China.

Government Contracting

In the world of government contracts, 2020 saw an increased focus on securing the supply chain and contractor cybersecurity. Two interim rules went into effect this year that i) increase the compliance obligations of federal contractors in connection with supply chain management and ii) require cybersecurity assessments of certain federal contractors' information networks.

A New Gating Function: Companies Using Huawei and Certain Other Chinese Telecommunications Products or Services May Be Ineligible for Federal Contracts

Beginning in August 2020, an interim rule went into effect that further addressed a perceived threat to the supply chain by certain China-based companies. In August 2019, the first set of contract clauses implementing Section 889(a)(1)(A) of the National Defense Authorization Act for Fiscal Year 2019 (NDAA) placed restrictions on the U.S. government's ability to purchase "covered telecommunications equipment or services" from Huawei and other identified China-based companies. In August 2020, the interim rule expanded these prohibitions (by amending FAR 52.204-25) to also prohibit the U.S. government from entering into a contract with an "entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system."

Therefore, in order to be eligible for federal contracts, contractors are now required to represent in the System for Award Management (SAM) whether, after a making a "reasonable inquiry," they "use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services" and to alert the U.S. government upon discovery of any such use in the course of a contract's performance. The certification pertains to *any* of the contractor's systems, regardless of whether those systems are used in the performance of federal contracts.

Subcontractors and suppliers do not have compliance obligations under the updated clauses, but as a practical matter, since a prime contractor is required to make the representation, they will most likely want to understand whether their suppliers and subcontractors are using any of the covered telecommunication equipment or services. Over the past several months, we have assisted clients in both drafting certifications for their subcontractors and suppliers to sign to support the clients' certifications, and in responding to requests for such certifications.

In order to make the certification, the rule established a "reasonable inquiry" standard. A "reasonable inquiry" means "an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity." Therefore, a "reasonable inquiry" can be based on information already possessed by the contractor, and there is no requirement to contact every supplier to determine the origin of certain equipment or services that the supplier may use.

A well-documented review, detailing the "reasonable inquiry," including documents reviewed and steps taken, should be conducted to support the required representation. In the immediate period of time after the rule's effectiveness, the U.S. government's expectations as to the scope of that reasonable inquiry may have been more limited than what they are today, and what they will be a year from now. Now that contractors have had time to absorb the impact of this rule, they are expected (per the rule) to develop compliance plans, including operationalizing the "reasonable inquiry" necessary to make the required representation.

Cybersecurity: A New Assessment Methodology and the Long-Awaited Rollout of CMMC

Many DOD contractors already have contracts which contain Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. This clause requires contractors that have "covered contractor information systems" to apply the cybersecurity requirements

of National Institute of Standards and Technology (NIST) Special Publication 800-171 (SP 800-171) to those systems. Under the clause, contractors may comply by having a system security plan in place to describe how the requirements of SP 800-171 are implemented along with "plans of action" to describe how and when any unimplemented security requirements will be met in the future.

But this interim rule changed things starting November 30, 2020, by instituting the DOD Assessment Methodology. Now, affected contractors that are required to implement SP 800-171 must conduct a "Basic" assessment and enter the results into the U.S. government's Supplier Performance Risk System (SPRS) as a condition of eligibility for the award of a new contract or the exercise of an option under an existing contract. A Basic assessment is a contractor's self-assessment of its implementation of SP 800-171 on each of its affected systems, and it includes a date by which it expects to be able to fully implement SP 800-171. Later, Medium and High assessments will be conducted by the U.S. government and, pursuant to DFARS 252.204-7020, contractors are required to provide access to their facilities, systems, and personnel for DOD to conduct that assessment. The level of assessment DOD may perform depends on the criticality of the program or sensitivity of information handled by the contractor.

In addition to the DOD Assessment Methodology, the interim rule also addresses the Cybersecurity Maturity Model Certificate (CMMC) Framework, which is a DOD certification process that measures a company's cybersecurity processes and practices beyond the requirements of SP 800-171. CMMC is intended to provide comfort that DOD contractors' systems are sufficient to protect unclassified information, such as Controlled Unclassified Information (CUI). By October 1, 2025, CMMC requirements should be present in virtually all DOD contracts. For now, very few contracts will include these CMMC requirements. Once CMMC is in effect, however, a new contract cannot be awarded, nor can a contract option be exercised, if the contractor does not have a current certification at the required CMMC level.

Both the DOD Assessment Methodology and CMMC are requirements that currently only apply to contracts with DOD entities; however, DOD often leads the U.S. government in this area, and it is likely other agencies will consider adopting their own versions of these cybersecurity assessment and review requirements in the future.

Conclusion

With a new incoming administration taking charge soon after the new year, the only certainty for 2021 is that technology companies and investors should expect further change in national security regulatory regimes. As the Biden team grapples with the U.S.'s policy toward China and other geopolitical competitors, the Wilson Sonsini National Security team will continue to keep clients abreast of the latest developments—please follow the team's presentations at Wilson Sonsini's On Demand Learning site for early predictions about changes in the coming year.

In the meantime, for more information about national security regulations, please contact Stephen Heifetz (sheifetz@wsgr.com); Joshua Gruenspecht (jgruenspecht@wsgr.com); Josephine Aiello LeBeau (jalbeau@wsgr.com); Melissa Mannino (mmannino@wsgr.com); Anne Seymour (aseymour@wsgr.com); or any member of the national security practice at Wilson Sonsini Goodrich & Rosati.

WILSON SONSINI

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

Austin Beijing Boston Brussels Hong Kong London Los Angeles New York Palo Alto San Diego San Francisco Seattle Shanghai Washington, DC Wilmington, DE