Business Law Update

Winter 2020

Mergers & Acquisitions

New CFIUS Regulations Will Cover Certain Non-Controlling Investments and Real Estate Transactions

By Samir D. Varma, Brent Connor and Scott E. Diamond*

The Committee on Foreign Investment in the United States (CFIUS), the interagency committee chaired by the secretary of the Treasury that is authorized to review transactions involving foreign investment in the United States for any national security concerns, continues to revise and update its operations and procedures due to the August 2018 enactment of the Foreign Investment Risk Review Modernization Act (FIRRMA). This law made various amendments to the CFIUS review process, including (1) creating a new pilot program requiring that certain proposed transactions be reported (see *Business Law Update*, Winter 2019), and (2) requiring regulations for the reporting of transactions involving foreign non-controlling investments and real estate transactions that previously fell outside CFIUS's jurisdiction.

After issuing proposed rulemakings in September 2019, the Department of the Treasury has recently finalized these regulations pertaining to "Certain Investments in the United States by Foreign Persons" and "Certain Transactions by Foreign Persons Involving Real Estate in the United States." These new regulations will become effective on February 13, 2020, and will vastly increase the scope of CFIUS reviews. While the majority of CFIUS filings will remain voluntary, it is expected that given the complexity in the regulations and growing national security sensitivity, parties involved in mergers, acquisitions and takeovers will increasingly seek CFIUS review and approval to receive "safe harbor," thus protecting their transactions from subsequent review or unwinding.

FIRRMA Provisions on Non-Controlling Investments

The new regulations expand CFIUS's jurisdiction to certain non-controlling investments that provide foreign persons access, rights or

Recent News & Related Articles

- Antitrust Agencies Release New Vertical Merger Guidelines
- DOL Finalizes Rule Redefining Joint Employer Status
- Renewed Restrictions on the Use of Mandatory Employment Arbitration Agreements
- Chemical Industry Regulatory Update - Jan. 2020
- Department of Justice Revises Export Control and Sanctions Enforcement Policy for Business Organizations
- DHS Warns Businesses About Potential Cyber Threats
- FAA Releases Long-Awaited Proposed Drone Remote Identification Rule

For more details on any of the topics covered in this *Business Law Update*, please contact the authors via the links at the end of each article or David R. Valz, editor-in-chief. For information on our Corporate Transactions & Securities practice, please contact Frank D. Chaiken, practice group leader.

involvement in certain U.S. businesses. Specifically, CFIUS review may be necessary when such non-controlling investments allow foreign persons: (1) access to material nonpublic technical information in the possession of the U.S. business, (2) membership or observer rights on the board of directors (or equivalent corporate body) of the U.S. business, or (3) involvement in substantive decision-making regarding actions related to critical technologies, critical infrastructure or sensitive personal data.

The term "material nonpublic information" includes, but is not limited to, information that provides knowledge, know-how, or understanding not available in the public domain, regarding the design, location or operation of critical infrastructure, or information not available in the public domain that is necessary to design, fabricate, develop, test or manufacture critical technology. The term "substantive decision-making" covers the process and decisions regarding pricing, sales and contracts; supply arrangements; corporate strategy and business development; research and development; access to critical technologies; physical and cybersecurity protocols; policies and procedures on the collection, use and storage of sensitive personal data; or strategic partnerships. The terms "critical infrastructure" and "critical technologies" remain broadly defined in the regulations to allow CFIUS latitude in its reviews. Critical infrastructure covers any systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems or assets would have a debilitating impact on U.S. national security. Critical technologies cover defense articles or services; certain items controlled for export purposes for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation or missile technology; regional stability; nuclear equipment; certain chemical agents and toxins; and emerging and foundational technologies. Under the new regulations, CFIUS has provided a list identifying covered investments in critical infrastructure and functions that would be sectors of concern in any national security review.

For the first time, under these new regulations, CFIUS has specific authority to review transactions in which the U.S. business maintains sensitive personal data of U.S. citizens that may be exploited in a manner that threatens national security. "Sensitive personal data" is defined to include 10 categories of data (including financial, geolocation and health data) maintained or collected by U.S. businesses that: (1) target or tailor products or services to sensitive populations, including U.S. military and certain federal employees; (2) collect or maintain such data on at least one million individuals; or (3) have a demonstrated business objective to maintain or collect such data on greater than one million individuals and such data is an integrated part of the U.S. business's primary products or services.

The regulations also create an exception from "covered investments" for certain foreign persons defined as "excepted investors." Any designation as an excepted investor will be based on ties to countries identified as "excepted foreign states," and those states' compliance with certain laws, orders and regulations similar to those of the United States concerning foreign investments assessed for national security purposes. CFIUS has initially identified Australia, Canada and the United Kingdom (including Northern Ireland) as excepted foreign states due to their "robust intelligence sharing and defense industrial base integration mechanisms with the United States." This list may be expanded in the future.

While the CFIUS process remains voluntary in most non-controlling investment instances, these new regulations clearly increase the scope of transactions which will be of interest to CFIUS. Note, however, that certain transactions involving critical technology may require a full notice or, at least, a short-form declaration in order to receive a potential "safe harbor" letter. Further, declarations will be required by CFIUS when a foreign government has a substantial interest (a voting interest of 25 percent or more by a foreign person or a voting interest of 49 percent or more by a foreign government in a foreign person) in the transaction.

FIRRMA Provisions on Real Estate Transactions

The new regulations also include provisions that allow CFIUS to review certain real estate transactions, including the purchase or lease by, or concession to, a foreign person of public or private real estate that is located near designated airports, maritime ports, military installations or sensitive government facilities, that could allow a foreign person the ability to collect intelligence on activities being conducted at such sites or could otherwise expose national security activities to foreign surveillance. To be a covered real estate

transaction, the involved foreign person would have to have certain property rights, such as (1) physical access to the real estate; (2) the right to exclude others from physically accessing the property; (3) the right to improve or develop the real estate; or (4) the right to attach fixed or immovable structures or objects to the property. CFIUS has provided a list of identified military installations and sites that would be locations of concern in any national security review and will rely on the Department of Transportation to identify any airports and maritime ports of concern.

These new CFIUS regulations covering foreign investment in real estate also set forth an exception for an "excepted real estate investor." Similar to "excepted investor," this category is based on ties to certain identified "excepted real estate foreign states." Again, CFIUS has initially identified Australia, Canada and the United Kingdom as eligible foreign states. There are also exceptions for real estate transactions in an "urbanized area" or "urban cluster," as defined by the Census Bureau. Generally, an urban cluster is viewed as a territory having a population of at least 2,500 persons but fewer than 50,000 persons, while an urbanized area is a location having a minimum of at least 50,000 individuals. Such exceptions would not be applicable to these areas when relevant ports and certain military installations are located in close proximity. Further exceptions will apply to real estate transactions involving a foreign person's purchase or lease of a single housing unit, or for transactions involving certain commercial office space in a multi-unit commercial office building.

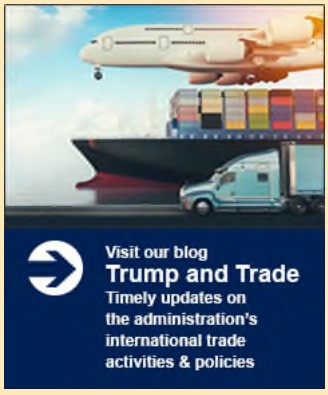
CFIUS has determined that there will be no mandatory filing requirements for real estate transactions. However, CFIUS has cautioned that only by filing a voluntary notice or a short-form declaration providing notification of a covered real estate transaction will the involved parties potentially qualify for a safe harbor letter.

Conclusion

With the new national security review regulations mandated by FIRRMA, CFIUS has an increased scope of transactions it can review and increased responsibilities, funding and staffing with which to operate. While continuing to welcome foreign investment in the United States, the CFIUS process has been modernized to address growing concerns over certain foreign states' intentions in their investments (i.e., obtaining access to certain technology, gaining insight into U.S. manufacturing processes and obtaining sensitive personal data). Noting that there is no specific list of countries from which investments will be prohibited, investments from **any** foreign persons remain potentially subject to CFIUS jurisdiction for national security purposes. These new regulations pertaining to non-controlling investments and certain real estate transactions are intended to clarify the areas of particular focus and concern for potential foreign investment, and to assist parties involved in foreign investment transactions as to whether they should consider submitting a notification to CFIUS.

Please contact Samir Varma, Brent Connor or Scott Diamond with any questions.

**Scott E. Diamond, Senior Legislative & Regulatory Policy Advisor in the International Trade group, is not licensed to practice law.*



TrumpandTrade.com

For the latest news and analysis in international trade law, please check out our blog, Trump and Trade. Recent updates include:

- Department of Justice Opines that Commerce Does Not Have to Release Section 232 Report on Imports of Automobiles and Automotive Parts
- The United States and China Sign "Phase One" Trade Agreement
- Congress Approves United States-Mexico-Canada Trade Agreement; President Trump Scheduled to Sign Legislation

To receive an email notification whenever a new post is published, please subscribe to the blog.

FTC Reiterates Rule Against HSR Avoidance Devices, Imposes Substantial Fines

By Mark R. Butscha, Jr. and Michael W. Jahnke

The Hart-Scott-Rodino Antitrust Improvements Act (HSR Act) generally requires parties to an acquisition valued above a certain threshold (currently $90 million) to notify the Federal Trade Commission (FTC) and Department of Justice (DOJ) of the pending transaction, and the proposed deal cannot close until 30 days after the notification is filed (or longer in the event of an investigation). Because of the potential cost and delay associated with HSR filings, parties scrutinize the arcane HSR rules to ensure that a filing is necessary.

Careful scrutiny of the rules is prudent, but parties should resist the temptation to restructure a transaction specifically to avoid the filing requirements of the HSR Act. The HSR Act prohibits "devices for avoidance" of HSR filing obligations (see 16 C.F.R. § 801.90). Specifically, parties cannot restructure a deal "for the purpose of avoiding the obligation to" make an HSR filing. Regardless of the technical structure of the deal, it is the substance that matters. The rule authorizes the FTC and DOJ to look past the form of a transaction "to the substance of the transaction" to determine if the parties are utilizing a device for avoidance.

The maximum civil penalty for an HSR violation is $42,530 per day (adjusted annually). In a November 2019 post on its *Competition Matters* blog, the FTC reiterated this rule, stating that "restructuring a deal to avoid or delay an HSR filing may subject the merging companies to substantial penalties if the restructured transaction still results in an acquisition by the A side." To illustrate the agency's view of the rule, the FTC highlighted a $5 million settlement reached in June 2019 with Canon Inc. and Toshiba Corporation of a claim that they had utilized an unlawful device for avoidance in connection with Canon's acquisition of a Toshiba subsidiary.

In the Canon/Toshiba case, the FTC filed a complaint in June 2019 alleging that the parties devised a scheme in March 2016 with no purpose other than to avoid an HSR filing obligation. The impetus behind the scheme was Toshiba's financial difficulties and the desire to close the deal prior to the end of fiscal year 2015 on March 31, 2016. The "device for avoidance" involved (1) restructuring the classes of ownership interests in the Toshiba subsidiary, (2) creating a third-party holding company, (3) transferring all the subsidiary's shares to the holding company for $900, and (4) transferring one non-voting share of the subsidiary to Canon for $6 billion. Technically or formalistically, no HSR filing was required for these transactions.

Nonetheless, the HSR Act does not elevate form over substance. As the FTC put it, "this convoluted series of transactions could not distort the reality of what was really going on." In the FTC's view, the "real purpose" of the transactions was revealed by the "end result," which was that Toshiba did not own its subsidiary, the new holding company had no incentive to operate the subsidiary it nominally acquired, and ownership would be surrendered to Canon. All of that would be accomplished without an HSR filing, the purpose of which is to preserve the status quo pending antitrust review. To settle the case, Canon and Toshiba agreed to pay $2.5 million apiece.

The Canon/Toshiba case illustrates how the FTC views the rule against devices for avoidance, and its blog post provides some additional guidance for parties to know where the FTC stands on this issue. The FTC rejected the view "that so long as there is a legitimate purpose for the overall structure of the transaction, then there is not a purpose to avoid." Rather, the FTC believes the relevant question is whether "the benefit that is the motive behind the transaction's structure result[s] from avoiding or delaying filing." If so, then "the structure is an avoidance device under the Rule." That is the case regardless of whether the motivation behind the device is anticompetitive. Conversely, if the structure of

the deal creates a benefit unrelated to HSR, such as a tax benefit, a delayed or avoided filing obligation may be "an incidental consequence of the structure" and not a device for avoidance.

In sum, it may be tempting to look for ways to use a "device for avoidance" to eliminate the expense and delay associated with an HSR filing, but parties should resist that temptation, so they do not subject themselves to substantial fines and penalties. Recent enforcement activity shows that the antitrust agencies remain attuned to this issue, and parties who are considering how to structure a potentially reportable transaction should seek advice from experienced HSR counsel to mitigate their antitrust risk.

Please contact Mark Butscha or Michael Jahnke with any questions.

Securities Quarterly – Winter 2020

Please visit our website to check out *Securities Quarterly*, our publication that provides updates and guidance on securities regulatory and compliance issues. In this edition, we look at developments during 2019 affecting periodic reporting requirements that public companies should consider as they prepare their Form 10-K filings for the fiscal year ended December 31, 2019.

Commercial Contracts

Don't Fall Asleep at the Wheel: Sellers Should Pay Close Attention to Limitations on Liability in Commercial Contracts

By Brendan J. McCarthy

If you're a prudent seller of goods or services, then, toward the end of each and every commercial contract to which you'll be a party, generally somewhere after the much-ballyhooed economic terms and right before the often overlooked miscellaneous terms, you're sure to include terms that limit your liability to the buyer. The importance of these terms cannot be overstated. They limit the extent to which you may be liable to the buyer in the event that the buyer suffers a loss and seeks indemnification from you under the contract. To go without them could leave you susceptible to unlimited liability. It is therefore incumbent on you, as the seller, to pay close attention to the language of these limitations on liability. If you are not careful, and rely too heavily on boilerplate provisions or permit a buyer to sneak in what may appear to be relatively innocuous revisions during negotiations, you might find that the very provisions that you thought would protect you from liability actually afford you little or no protection at all. The following are three key areas where something might fall through the cracks if you're not awake at the wheel:

1. Not Adequately Disclaiming Damages for Lost Profits

The prudent seller will include a provision disclaiming liability for certain types of damages in a commercial contract. A typical damages disclaimer will preclude the buyer from seeking and recovering consequential damages that may flow from the breach that is the basis of the claim. But what happens if the buyer is successful in arguing that lost profits, often considered consequential damages, are, in fact, direct damages because they are the natural and probable consequence of the breach? If you have not expressly disclaimed liability for lost profits (both direct and indirect) or made clear that lost profits (both direct and indirect) are considered consequential damages under the contract, then you might just find yourself out of luck. And lost profits could prove to be a very significant amount. Therefore, you should be careful to either expressly disclaim liability for both direct and indirect lost profits or define

"consequential damages" so that the term includes both direct and indirect lost profits (and then be sure to disclaim liability for consequential damages) in order to avoid potentially being on the hook for damages for lost profits.

2. Not Adequately Defining the Cap When It's Not a Set Dollar Amount

One of the most important things that the prudent seller can do to limit liability under a commercial contract is to include a cap on liability, which sets forth the maximum amount that the buyer can recover under the contract. If the cap is a set dollar amount, then the maximum amount is clear and obvious. But what if you tied the cap to a percentage of amounts paid to you under the contract for some period preceding the event giving rise to the claim? If you have not made clear that there is an overall cap that can limit your aggregate liability, then defining the cap in such a way may inadvertently allow it to reset each and every time that there is a period of time during which there are no events giving rise to successful claims that are counted toward its satisfaction. Therefore, you should be careful when crafting the cap on liability and make sure that if you tie it to anything other than a set dollar amount, you consider the possibility that it could reset under certain circumstances.

3. Permitting All Indemnification to Be Carved Out of Disclaimer and/or Cap

Despite including a damages disclaimer and a cap on liability in a commercial contract, the prudent seller can expect that the buyer will fight hard to carve items out from them. One item that the buyer will undoubtedly try to carve out is indemnification. If the indemnity you are going to give the buyer is wide-ranging, then you may inadvertently nullify the damages disclaimer and the cap on liability if you permit all indemnification to be carved out, because there would be virtually nothing stopping the buyer from seeking and recovering any type of damages and any amount of money so long as the claim can be couched in indemnification. If, however, the indemnity you are going to give the buyer is sufficiently limited, then you might be able to get comfortable carving out all indemnification. Therefore, to get the true benefit of the damages disclaimer and the cap on liability, you should be careful to limit what types of indemnification, if any, will be permitted to be carved out from them.

These are just a few of the ways that you, the seller of goods or services, might find yourself not as protected as you thought you were by the limitations on liability that you made sure to include in your commercial contract. Do not let yourself fall asleep at the wheel during negotiations with the buyer and fall victim to boilerplate provisions that do not adequately limit your liability or a savvy buyer that lightly revises your limitations on liability in a way that severely undercuts or nullifies them.

With any questions, please contact Brendan McCarthy.

Labor & Employment Breakfast Briefing

Tuesday, February 18 – Dayton

8:00 - 8:30 a.m. – Breakfast & registration | **8:30 - 10:30 a.m.** – Program

Please join us for a program focused on new employment regulations, initiatives and trends. We will provide an overview of hot topics and a preview of what to expect in 2020. We will also offer a road map of updates to consider for your organization's employment policies. Key topics include:

- The watch for landmark Supreme Court decisions on LGBTQ discrimination issues
- #MeToo implications in the workplace
- ADA and leave administration updates
- Trends in paid sick leave and unlimited PTO policies
- New wage theft notice laws
- Steps employers can take to prevent workplace violence

Our presenter will be Deborah S. Brenneman, a partner in Thompson Hine's Labor & Employment and Business Litigation practice groups.

For more information, or to register, please visit ThompsonHine.com/Events.

Small Businesses

Changes to the Bankruptcy Code Will Favor Small Businesses

By Jonathan Hawkins

Effective February 19, 2020, the U.S. Bankruptcy Code (Code) will be amended by the Small Business Reorganization Act (SBRA). The overall purpose of the amendments is to increase the ability of a small business to reorganize, but there are other changes intended to shield small business creditors from the effects of larger bankruptcy cases.

The SBRA follows Code amendments from 2005 that were intended to enhance small business flexibility in using the chapter 11 process to reorganize. However, in practice, small businesses' ability to use the 2005 changes remained hampered by many requirements found in large business bankruptcies. Of critical importance, the SBRA eliminates the "absolute priority rule" which requires that, absent consent, classes of equity retain nothing if senior classes – i.e., creditors – were not paid in full. Now, shareholders of small businesses can retain their interests if the outcome is better for creditors than a hypothetical liquidation of the business and all available net income is devoted to repaying creditors.

Other major changes include the automatic appointment of a "subchapter V" trustee, who controls disbursements, and the expectation that a plan be proposed within 90 days of the filing of the bankruptcy. The accelerated timeline is intended to keep the costs of expensive bankruptcy case administration down while increasing the likelihood of successful reorganization. Presently, the threshold for a "small business" debtor is limited to those persons or entities that have approximately $2.7 million in commercial debt. However, proposals to expand the debt limit to $10 million are under consideration.

The SBRA also adds hurdles to debtors or trustees pursuing preference actions. One critical addition to the Code requires the preference plaintiff to conduct "reasonable due diligence in the circumstances of the case" and to "tak[e] into account a party's known or reasonably knowable affirmative defenses." While it remains to be seen the extent to which these provisions will reduce litigation, in practice, this provision should reduce the practice seen frequently in large bankruptcy cases where litigation or chapter 7 trustees "shoot first and ask questions later."

Finally, the SBRA modifies venue provisions, requiring cases asserting a preference or similar "clawback" claim less than $25,000 to be filed in the district in which the defendant resides. Rather than being faced with the decision to defend a small claim in a distant forum or lose by default, creditors that receive payment prior to bankruptcy for less than $25,000 can rest easy knowing it is the debtor or litigation trustee that needs to consider whether pursuing the claim is worthwhile.

Please contact Jon Hawkins with any questions.

Government Contracts

Defense Department Implementing New Cybersecurity Certifications for the Industrial Base

By Joseph R. Berger and Tom Mason

The U.S. Department of Defense is preparing to implement its Cybersecurity Maturity Model Certification (CMMC) program for contractors this year, which will ultimately require third party certifications for more than 300,000 companies in the DOD supply chain. DOD published the preliminary versions of the draft CMMC model framework late last year along with an overview briefing on the CMMC, and expects to release Version 1.0 this month (January 2020). The CMMC enforcement mechanism will build upon, and significantly add to, the current DOD cybersecurity requirements, which include DFARS 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting) and the incorporated requirements developed by the National Institute of Standards and Technology (NIST). Additional parameters for the CMMC program were adopted in the National Defense Authorization Act (NDAA) for Fiscal Year 2020.

CMMC Program Background

The Office of the Under Secretary of Defense for Acquisition & Sustainment (OUSD(A&S)) worked throughout 2019 with DOD stakeholders, federally funded research and development centers, the Johns Hopkins University Applied Physics Laboratory and the Carnegie Mellon University Software Engineering Institute to "review and combine various cybersecurity standards into one unified standard for cybersecurity." The OUSD(A&S) website provides the latest news and updates.

OUSD(A&S) has explained that the CMMC will become a requirement in DOD procurements through solicitation proposal instructions and evaluation criteria, which will set the required CMMC level for specific contracts at Levels 1-5. OUSD(A&S) has also announced that cybersecurity costs will be considered allowable costs by DOD. According to the OUSD(A&S) website, "the CMMC effort builds upon existing regulation (DFARS 252.204-7012) that is based on trust by adding a verification component[.]"

According to the OUSD(A&S) briefing, CMMC Rev. 1.0 is expected to be released in January 2020, and its requirements will be included in requests for information (RFIs) as soon as June 2020 and requests for proposals (RFPs) in the fall. OUSD(A&S) has stated that "the goal is for CMMC to be cost-effective and affordable for small businesses to implement at the lower CMMC levels."

Last year OUSD(A&S) issued an RFI to interested parties concerning the CMMC Accreditation Body. According to OUSD(A&S), the CMMC Accreditation Body will provide oversight for CMMC accreditations and assessments, including quality control, training, dispute resolution, and database and records management. The Accreditation Body will liaise with DOD regarding the CMMC assessments of individual companies.

According to the RFI, to obtain a CMMC certification, and to request and schedule a CMMC assessment, companies will coordinate directly with an independent CMMC Third-Party Assessment Organization (C3PAO) that has been accredited by the CMMC Accreditation Body. Upon successful demonstration of the appropriate capabilities and organizational maturity, the organization will receive the corresponding CMMC level certification. DOD's working estimate for the number of organizations requiring CMMC certifications is 300,000, "with a very high percentage of those companies in the micro-, small-, and mid-size range." Each assessment "will be conducted by a credentialed independent assessor working for an accredited C3PAO under the oversight of the CMMC Accreditation Body." DOD's goal is for the Accreditation Body to be established and prepared to certify candidate C3PAOs in the spring of 2020.

CMMC Adopted in NDAA for FY 2020

The CMMC program as planned by DOD is consistent with Section 1648 of the NDAA for Fiscal Year 2020, which endorses the CMMC and requires other DOD efforts to

improve the cybersecurity of the U.S. defense industrial base (DIB). Section 1648 requires the secretary of Defense to develop a comprehensive framework to enhance the cybersecurity of the DIB no later than February 1, 2020. This will include "the responsibilities of the prime contractors, and all subcontractors in the supply chain, for implementing the required cybersecurity standards, regulations, metrics, ratings, third-party certifications, and requirements identified[.]" The secretary is required to consider "risk-based methodologies, standards, metrics, and tiered cybersecurity requirements for the defense industrial base, including third-party certifications such as the Cybersecurity Maturity Model Certification pilot program, as the basis for a mandatory Department standard."

CMMC Model Requirements

The CMMC will be a unified cybersecurity standard for DOD acquisitions to reduce "exfiltration" of controlled unclassified information from the DIB. The CMMC combines various cybersecurity standards and best practices, which are mapped across several maturity levels that range from basic cyber hygiene to advanced.

The draft CMMC model framework released last year consisted of 17 cybersecurity domains, which are based on "best practices." The CMMC domains are comprised of capabilities, which are further comprised of practices and processes, which are mapped to CMMC Levels 1 through 5. The capabilities, practices and processes are each set forth in the comprehensive draft CMMC model framework. Most of the domains overlap with security requirements in NIST SP 800-171 Rev. 1 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations).

The new CMMC requirements also include additional practices derived from a variety of content sources. Level 1 includes basic cybersecurity that is achievable for small companies. Level 3 includes coverage of all controls required by NIST SP 800-171 Rev. 1, as well as additional practices. Level 5 includes advanced cybersecurity practices reserved for the most critical systems.

According to the OUSD(A&S) briefing, examples of Level 1 practices include FAR requirements, antivirus protection, ad hoc incident response and ad hoc cybersecurity governance. Examples of Level 2 practices include risk management, awareness and training, and backups and security continuity. Examples of Level 3 practices include all NIST SP 800-171 Rev. 1 requirements, an Information Security Continuity Plan and communication of threat information to key stakeholders. Levels 4 and 5 are "targeted toward a small subset of the DIB sector that supports DOD critical programs and technologies."

CMMC Will Add to Existing Auditing, Investigations and Enforcement

The CMMC program is expected to bring a new enforcement mechanism to cybersecurity that will enhance security for contractors and the industrial base, and help DOD avoid future losses to cyber breaches. Cybersecurity can also be expected to be an increasing target for current and future auditing, investigations and other enforcement efforts. In a January 2019 memorandum issued by the under secretary of Defense for Acquisition and Sustainment, DOD instructed the Defense Contract Management Agency to include in its audit of a contractor's purchasing system a review of compliance with the cybersecurity requirements of DFARS 252.204-7012 and NIST SP 800-171, for both the contractor and its "Tier 1 Level Suppliers."

Developments within the last year also include False Claims Act (FCA) and other enforcement actions. In May 2019, a district court denied a motion to dismiss an FCA complaint against a major defense contractor alleging violations of the cybersecurity requirements of DFARS 252.204-7012 and a related NASA cybersecurity clause. In June 2019, U.S. Customs and Border Protection suspended a contractor following a high-profile data breach. And in July 2019, it was announced that a major IT company had agreed to pay $8.6 million to settle DOJ and relator allegations that it had violated the FCA by selling video surveillance equipment with cybersecurity flaws to federal agencies. These events, as well as continuing news of cyber breaches and cyber advances by competitor nations, serve as a reminder that even as DOD implements the new enforcement and certification mechanisms, contractors must continue to devote substantial and increasing resources toward compliance with the current cybersecurity regulations, including the comprehensive DFARS and NIST requirements.

Please contact Joe Berger or Tom Mason with any questions.