Wiley Rein LLP

GOVERNMENT CONTRACTS ISSUE UPDATE

September 2018

National Defense Authorization Act for Fiscal Year 2019 Includes Acquisition Reforms That Contractors Should Be Aware Of

By Tracye Winfrey Howard and Kendra P. Norwood

On August 13, 2018, President Trump signed into law the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019, which sets federal funding levels and outlines the spending and policy priorities for the U.S. Department of Defense (DOD). Although the NDAA does not include sweeping acquisition reforms, it does include several provisions that will directly affect contractors. These changes include placing additional limits on sole-source and lowest price technically acceptable (LPTA) contracting, revising the definition of "commercial item" to separately address products and services, requiring additional justifications and approvals for exercising multi-year contract authority or withholding consent to subcontract, directing full and open competition for the forthcoming GSA e-Commerce Portal, and providing exceptions for price competition in the award of indefinite-delivery indefinite-quantity (IDIQ) contracts. Several of these changes were recommended in early reports by the "Section 809 Panel" on DOD acquisition reform that was established in the FY 2016 NDAA. We expect the Section 809 Panel to propose more comprehensive acquisition reforms in its final report at the end of the year, which Congress is likely to address in the FY 2020 NDAA.

continued on page 4

Summer School: Recent Bid Protest Decisions on Timing Issues That Business Teams and In-House Counsel Need to Know

By Kara M. Sacilotto and Craig Smith

The Government Accountability Office (GAO) issued decisions over the summer that make up a short course on proposal- and protest-related deadlines. For proposal/capture teams and in-house counsel involved in the debriefing and protest decision-making process, this article highlights two lessons involving debriefing requests and DOD's new "enhanced" debriefing procedures. These decisions reinforce a basic tenet of protest procedures: late still means late.

continued on page 7

ALSO IN THIS ISSUE

MITRE Report Recommends Critical Changes to Supply Chain Security

By Moshe B. Broder

In August 2018, MITRE Corporation released a report recommending significant enterprise-wide changes to cyber and supply chain security, including changes in the role of cybersecurity in the procurement process. The report, "Deliver Uncompromised, A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War," is the latest cybersecurity development for defense contractors, and a sign of further changes to come.

The "Deliver Uncompromised" MITRE Report

The genesis of the MITRE report dates to 2010, when government officials and industry executives began publicly discussing concerns about the federal Government's tolerance for contractors who repeatedly delivered "compromised" capabilities to the DOD and Intelligence Community (IC). The report states that many DOD agencies and programs have already been compromised. MITRE's study focused initially on software integrity, but widened to include supply chain security, including major weapon systems. The report highlights the changing character of war, as adversaries strategically shift the paradigm in which they engage the United States from traditional kinetic actions to non-kinetic blended operations that take place in the supply chain, cyber, and human intelligence domains. Adversaries avoid fighting in areas of traditional U.S. strength, and seek to exploit asymmetric capabilities to defeat technological advances. This asymmetric engagement requires careful consideration of supply chain security and cybersecurity for DOD and its contractors.

The stated objective of the "Deliver Uncompromised" report is to "deliver warfighting capabilities to Operating Forces without their critical information and/or technology being wittingly or unwittingly lost, stolen, denied, degraded, or inappropriately given away or sold." The report acknowledges several structural challenges to achieving this objective. Notably, the report alleges that "overreliance on 'trust,' in dealing with contractors . . . has encouraged a compliance-oriented approach to security—doing just enough to meet the 'minimum' while doubting that sufficiency will ever be evaluated." The report recommends a fundamental change from the current trust-based system to one based on compliance with expert, independent industry standards.

The report recommends that "product integrity, data security, and supply chain assurance should become ***key contract award criteria***." To that end, the report recommends a number of significant Courses of Action (COA), including several that, if implemented, would have considerable impact on government contractors. The first and most significant COA would be to elevate security to a "primary metric" in DOD acquisition and sustainment. As the report explained, DOD currently measures program success and competitiveness largely using a set of well-established cost, schedule, and performance objectives. These acquisition parameters, however, fail to account for the true cost and risk of capability ownership, including system integrity and mission assurance, of which supply chain and cybersecurity are key components. The report calls for security to be recognized as a fourth pillar in the acquisition process, and envisions security evaluations taking place in three dimensions: by the Government on contractors currently performing on other contracts;

continued on page 3

continued from page 2

by an independent entity that will prepare and make available System Integrity Scores (SIS), akin to the "Moody's" model; and by privately procured monitoring services. The report places considerable emphasis on the role of the SIS, which is envisioned as a public-private entity that could act as an accrediting intermediary, and whose ratings could be used to qualify and evaluate offerors in the source selection process. These changes, according to the report, should incentivize contractors to invest more heavily in cyber and supply chain security. Relatedly, the report recommends reducing some of the transparency in acquisitions, particularly in acquisitions of high-impact programs and in areas with heightened cyber and supply chain risk, on the basis that "massive amounts" of information regarding these programs has been exposed to and exploited by adversaries.

If these changes are implemented, they will likely create new urgency for successfully demonstrating compliance with existing security standards, such as those required in DFARS clause 252.204-7012 and outlined in NIST SP 800-171, in addition to demonstrating strengths beyond the minimal levels of acceptability. Since the report envisions broader government review and assessment of DFARS 252.204-7012 compliance, it may pave the way for compliance audits and enforcement actions. And, to the extent that cyber and supply chain security become more prevalent in the source selection process, contractors can expect to see these issues explored more frequently in bid protest litigation.

The report contains several other recommended COAs. For example, it recommends the creation of a jointly-governed inter-agency entity, called the National Supply Chain Intelligence Center, which can aggregate and analyze disparate data and disseminate reports to at-risk industry partners. The report recommends requiring the application of automated validating tools and software to conduct independent continuous monitoring for nefarious behavior. The report also calls for DOD to spearhead advocacy efforts for litigation reform and liability protection for contractors, especially for those involved in software development. The report acknowledged that contractors often hesitate to share relevant threat information with the Government out of concern that they could expose themselves to liability, in part because the Government may be unable to protect the contractor's identity or the information it provides. The report also raised the possibility that companies designated as "trusted suppliers" would be required to agree to a greater set of disclosure obligations and information sharing. Finally, the report acknowledges that smaller subcontractors who are deeper in the supply chain are more likely to be attractive targets for hostile actors, but they may lack the resources to properly defend themselves. To mitigate that risk, the report recommends tax incentives, akin to those provided to businesses that invest in renewable energy, and private insurance initiatives to spur development for smaller companies.

In summary, the MITRE report contains several significant and wide-ranging proposals for changes to the role of cybersecurity in government acquisition and administration of contracts. While it remains to be seen which changes will be implemented, these proposals establish a roadmap for an increasingly significant role that cybersecurity and supply chain security will play for federal contractors.

For more information, please contact:

Moshe B. Broder: 202.719.4186
mbroder@wileyrein.com

The FY 2019 NDAA also requires DOD to submit reports to Congress on high-profile issues such as "second bite at the apple" bid protests filed at both the Government Accountability Office (GAO) and the U.S. Court of Federal Claims (COFC), the use of Other Transaction Authority, and a mandated pilot program to accelerate contracting and pricing processes. These and other provisions are summarized below. In addition to the acquisition reforms, the policy provisions in the NDAA also enact significant changes regarding **cybersecurity**, **foreign ownership of U.S. companies**, and export controls.

Commercial Item Contracting (Sections 836-838)

The FY 2019 NDAA revises the definition of "commercial item" by separating it into two new definitions: "commercial product" and "commercial service." Despite the new nomenclature, the scope and definitions of the two concepts remain largely unchanged. The term "commercial product" is consistent with the first few prongs of the current commercial item definition. Thus, a "commercial product" will be one that is of a type customarily used by the general public or nongovernmental entities for nongovernmental purposes and either (1) has been sold, leased, licensed or offered to the general public, in its original or slightly modified state, or (2) is not yet available but will be in time to satisfy the Government's requirements. Also included in the definition of "commercial products" are nondevelopmental items that were developed exclusively at private expense and have been sold competitively to multiple state, local, or foreign governments. "Commercial services" will include services provided to the public, sold competitively in substantial quantities in the commercial marketplace, and procured by the federal Government for support of commercial products. This is similar to the current services prong of the "commercial item" definition.

The NDAA also amends other related definitions and provisions of the acquisition statutes to substitute "commercial product" or "commercial service" for "commercial item." The new definitions will take effect on January 1, 2020, and DOD must submit a detailed implementation plan to Congress by April 1, 2019. The Federal Acquisition Regulation (FAR) and agency-specific supplements will require significant updates to incorporate the new definitions, and DOD and the FAR Council could use that opportunity to address other un-related changes to the relevant regulations. Industry should pay close attention to how these changes are implemented to identify potential unexpected changes.

In response to the Section 809 Panel's recommendations for streamlining procurement of commercial products and services, the FY 2019 NDAA also limits the applicability of certain executive orders and procurement regulations to commercial products and services. The NDAA also requires FAR Council to review the procurement regulations applicable to commercial products and services and recommend exemptions from FAR requirements unless there is a statutory reason to not provide an exemption.

Increase in DOD Micro-Purchase Threshold (Section 821)

The FY 2019 NDAA increases the DOD micro-purchase limit from $5,000 to $10,000, making the threshold the same for all federal government agencies. Congress elected not to

continued on page 5

further increase the micro-purchase threshold to $25,000 for purchases through the new e-commerce portal, which GSA and OMB had requested to incentivize broader participation from vendors and government agencies.

GSA e-Commerce Portal Competition (Section 838)

The FY 2019 NDAA authorizes GSA to develop procedures for procurements through the e-commerce portal. Under those procedures, a procurement will satisfy competition requirements if there are at least two suppliers that offer comparable products on the portal. The NDAA also expresses the sense of Congress that the portal must enhance competition, expedite procurement, ensure a reasonable price for commercial products, be implemented through multiple contracts with multiple portal providers, and safeguard data from suppliers and other e-commerce vendors to ensure the data is not used for pricing or marketing purposes or to obtain a competitive advantage.

Bid Protest Study, Tracking and Expedited Process (Section 822)

In response to a long-standing DOD request to revise the jurisdiction of the COFC to eliminate so-called "second bite at the apple" bid protests, i.e., successive protests at GAO and the COFC involving the same DOD contract award or proposed award, the FY 2019 NDAA instead requires DOD to conduct a study of the frequency, duration, and collateral impacts of such protests. The study must identify and analyze:

- The number of protests filed at both venues, the results of each, and the number of times GAO and the COFC reached different outcomes;
- The average and median lengths of time consumed by each stage of the litigation;
- The number of protests where performance was stayed or enjoined, and for how long, as well as whether the Government's requirement went unfulfilled during the stay or was obtained through another contract vehicle or in-house;
- Whether any monetary damages were awarded and, if so, in what amount; and
- For each protest, whether the protester was an incumbent contractor and whether the protester was a small or large business.

DOD must also establish a data collection system to better track and analyze GAO and COFC bid protest trends. The NDAA also directs DOD to develop an expedited bid protest process for DOD contracts valued at less than $100,000, which seems likely to increase the number of protests related to those low dollar-value procurements. DOD must submit a report to Congress on the expedited process by May 1, 2019, with implementation by December 1, 2019.

Technical Data Rights (Section 865-866)

The FY 2019 NDAA clarifies that the Government may continue to exercise rights in technical data while a dispute over the nature and scope of the Government's data rights is pending before a Board of Contract Appeals or the COFC, so long as the Secretary of Defense provides a written determination that "compelling mission readiness requirements" will not permit awaiting the final decision of the Board or Court. The Secretary of Defense must also develop policies on the negotiation

continued on page 6

of technical data rights for noncommercial software in the event of a protest or the replacement of an incumbent contractor. DOD must also develop training and guidelines on the use of Specially Negotiated Licenses for major weapons systems to address the numerous interpretations of those licenses within Government and industry.

Other Transaction Reporting (Sections 211, 873)

Congress continued its focus on enhancing the use of Other Transaction Agreements (OTAs). As a follow-on to the preference for OTAs established in the FY 2018 NDAA, the FY 2019 NDAA requires DOD to collect and analyze data related to the Department's use of OTAs, report annually to Congress on the data collected, and update policy and guidance related to the use of OTAs. The report to Congress must also identify any successes or challenges associated with DOD's use of OTAs.

The FY 2019 NDAA also revised the statutory authority for follow-on production OTAs, to allow them even if predecessor prototype projects had not been completed. This change was a direct response to GAO's bid protest decision in *Oracle America, Inc.*, B-416061 (May 31, 2018), which sustained a protest because the agency had executed a follow-on production OTA without first completing the prototype projects.

Task Order Price Competition (Section 876)

The FY 2019 NDAA provides several exceptions that will allow DOD agencies to award multiple award IDIQ contracts, including those under the Federal Supply Schedule, to acquire services where price is not necessarily an evaluation factor. Under these exceptions, DOD agencies may award un-priced contracts and then establish fair and reasonable prices through competition at the task order level.

LPTA Source Selection Policy (Section 880)

As a follow-on to the lowest price technically acceptable (LPTA) source selection limitations for DOD in the FY 2018 NDAA, the FY 2019 NDAA expands those restrictions government-wide by requiring a new FAR provision to limit the use of LPTA procurements. LPTA procurements will be authorized only if agencies clearly describe the minimum requirements, performance objectives, and standards that will be used to evaluate proposals. Agencies must also make a determination that any proposed technical approach would require little to no subjective judgment to evaluate and that the agency expects little to no value from an offeror exceeding the minimum requirements. The FAR provision must also make clear that LPTA source selections should be avoided to the maximum extent possible for procurements of services such as information technology, health care, and cybersecurity, as well as personal protective equipment and contingency operations. Additionally, the NDAA directs GAO to develop a methodology that would provide insight into the specific LPTA source selection criteria agencies continue to employ.

Pilot Program to Accelerate Contracting and Pricing Processes (Section 890)

The FY 2019 NDAA requires DOD to establish a pilot program to "reform and accelerate" the contracting process for contracts exceeding $50 million by (1) basing price reasonableness determinations on actual cost and pricing data for DOD purchases of

continued on page 21

What Time Is a Debriefing Request Due?

For GAO protest filings, 5:30 p.m. Eastern is ingrained as the default deadline. But what about protest-related submissions to agencies, such as the written request for a debriefing under FAR 15.506(a)(1) that must be submitted within three days after receiving a notice that an offeror was not selected for award? According to GAO: unless another time is stated, meeting a filing deadline means receipt by the agency in full ***by 4:30 p.m.*** in the agency's local time.

In ***Exceptional Software Strategies, Inc.*, B-416232, July 12, 2018**, an agency notified ESSI of its exclusion from the competitive range on a Thursday; the notice explained the agency's reasons for the exclusion. At 5:24 p.m. the following Monday, the agency received an email from ESSI requesting a debriefing. Two weeks later, the agency furnished a debriefing that included an account of the reasons for exclusion that was "nearly verbatim" of the initial notice.

Although ESSI subsequently filed a protest within ten days after receiving the debriefing, GAO dismissed the protest as untimely because it was filed more than ten days after ESSI first learned the reasons for its exclusion from the competitive range (via the exclusion notice). GAO determined that the safe harbor in GAO bid protest rule 4 C.F.R. § 21.2(a)(2) for protests filed within ten days of any "required" debriefing did not apply, because the debriefing the agency furnished to ESSI was not "required."

Under FAR 15.505(a)(1), a pre-award debriefing is "required" only if the offeror submits a written request for one to the contracting officer within three days of receiving the exclusion notice. Here, due to the weekend, ESSI had until the Monday following receipt of the notice of exclusion to submit the written request for a required debriefing. So the question boiled down to whether the submission of that request at 5:24 p.m. on the third day was timely or late.

FAR 15.505 does not specify a time deadline for debriefing requests, so GAO looked to FAR Subpart 33.1, which governs protest procedures. FAR 33.101 defines "filed" to mean an agency's complete receipt of a document "before its close of business." Except when another time is stated, FAR 33.101 presumes "4:30 p.m. local time" to be the "agency close of business."

Applying that rule to the debriefing request, GAO determined that the submission at 5:24 p.m. local time on the third day was too late to be considered submitted (or "filed") that day, and thus was not timely submitted within three days. Consequently, the debriefing the agency ultimately furnished was not a "required" debriefing that extended ESSI's period for filing a timely protest until ten days after the debriefing. And, because ESSI did not receive any new information in the debriefing that it had not already learned from the initial notice, the protest was dismissed as untimely.

Lesson learned: When it comes to debriefings, avoid any timing risk and submit your written request right away but, if you must submit the request on the third day, be sure to submit before 4:30 p.m. local time for the agency. In cases where the contracting activity may be overseas, that deadline could be earlier than anticipated. ***The 4:30 p.m. deadline also likely applies to agency-level protests***,

continued on page 8

which are subject to the same deadlines in FAR Subpart 33.1 that GAO applied in *Exceptional Software Strategies*.

"Enhanced Debriefings" are not Endless Debriefings

Another contractor ran afoul of protest deadlines by taking too many liberties with the **March 22, 2018 DOD class deviation** implementing Section 818 of the FY 2018 NDAA. The class deviation prescribes "enhanced debriefings" for disappointed offerors and states that contracting officers should inform these offerors that they can submit additional questions related to the debriefing within two business days of receiving the debriefing. The debriefing is to be held open until the agency provides its written responses.

In ***State Women Corp.*, B-416510, July 12, 2018**, State Women Corp. (SWC) lost a competition to construct a new morgue and visitation center at the Kabul National Military Hospital in Afghanistan. After SWC's timely request, the Army Corps of Engineers provided a written debriefing that invited SWC to submit any additional questions relating to the debriefing within the class deviation's two-day window.

SWC timely submitted written questions, and the Corps responded in writing within a few days. The Corps' response expressly stated that the debriefing was "hereby concluded." But the following week, SWC submitted additional questions, which the Corps responded to almost two weeks later. Four days after receiving these additional responses—but more than three weeks after receiving answers to its first round of follow-up questions—SWC filed a protest at GAO.

The Corps filed a motion to dismiss, arguing that to be timely a protest must be filed "[f]ive days after the Government delivers its written response to additional questions by the unsuccessful offeror," and citing text in the class deviation that establishes when an agency must stay performance of the awarded contract in accordance with the Competition in Contracting Act (CICA). SWC responded that its protest was timely because it was filed within five days of receiving the Corps' response to its second set of questions.

GAO found the protest untimely, but not for the reasons the Corps advanced. As GAO noted, a timely protest must be filed within ten days of a required debriefing. The enhanced debriefing class deviation does not change GAO's deadlines for a timely protest—the five-day deadline cited by the agency determines only whether the protest filing triggers an automatic stay of performance under CICA (an issue generally outside GAO's purview). The real timeliness issue was that SWC's protest was not based on new information learned from the agency's responses to SWC's second round of debriefing follow-up questions, so the protest was not filed within ten days of the conclusion of SWC's required debriefing.

For GAO, the only question was whether the agency held the debriefing open after it responded to SWC's first round of debriefing questions. Because the Corps specifically stated that the debriefing was "hereby concluded" when it responded to the first round of questions, GAO concluded that the debriefing did not remain open for subsequent rounds of additional questions. GAO explained that SWC's dissatisfaction with its debriefing, and its posing continued questions to the agency, did not extend the time for filing a

continued on page 9

protest based on the debriefing. GAO further found no support in either FAR 15.506(d) or the class deviation "for the proposition that an offeror is entitled to multiple rounds of postaward debriefing questions."

Lesson learned: Be thankful for what you get. Under the enhanced debriefing class deviation, a disappointed offeror for a DOD competition subject to FAR 15.506(d) should be provided at least one opportunity to submit questions and receive a written response. Although that offeror might continue to ask questions, and the agency might continue to entertain them, if the agency says the debriefing is over, it is over. And, if the agency does not indicate one way or the other whether the debriefing remains open, it is best to ask and get an express answer that the agency is holding the debriefing open for additional rounds of questions. Although GAO will resolve ambiguities about timing in favor of the protester, *see Harris IT Servs. Corp.*, B-406067, Jan. 27, 2012, it is better to be safe than sorry.

For more information, please contact:

Kara M. Sacilotto
202.719.7107
ksacilotto@wileyrein.com

Craig Smith
202.719.7297
csmith@wileyrein.com

Kara Sacilotto Begins Term as ABA Section Chair

In August, Kara Sacilotto began her term as Chair of the ABA Section of Public Contract Law. Kara looks forward to working with all members to advance the Section's mission of improving the procurement system and providing professional development opportunities for procurement attorneys and affiliated professionals. If you have ideas on how to improve the Section, please call Kara directly at 202.719.7107. And don't forget to join the Section's **LinkedIn group**.

Recent Legislative Proposals Seek to Address Supply Chain Risks in Information Technology Procurements

By Nina S. Samuels

The White House and Congress recently proposed legislation addressing supply chain risks in information technology (IT) procurement. Two legislative proposals, the Federal Acquisition Supply Chain Security Act of 2018 (FASCA) and Federal Information Technology Supply Chain Risk Management Improvement Act, are discussed below. These legislative initiatives are in addition to the policy developments addressed in the report by the MITRE Corporation, addressed separately in this Newsletter.

The Federal Acquisition Supply Chain Security Act

On June 19, 2018, Senators James Lankford, R-OK, and Claire McCaskill, D-MO, introduced FASCA. The bill would, among others, create a Federal Acquisition Security Council comprised of seven agencies, with the authority to exclude sources from federal acquisitions for IT and supply chain security purposes. The Council would have a number of different functions, including: developing criteria and processes for assessing supply chain threats and vulnerabilities posed by the acquisition of IT to national security and the public interest; issuing guidance to executive agencies for incorporating information relating to supply chain risks into procurement decisions for the protection of national security and the public interest; and determining whether the exclusion of a source by one executive agency for IT security purposes should apply to all executive agencies.

FASCA would also extend to civilian agencies the authority to take procurement actions based on IT and supply chain security risks, similar to the authority previously granted to DOD in Section 806 of the FY 2011 NDAA, which is implemented in DFARS Subpart 239.73 and was recently reauthorized in the FY 2019 NDAA. This extension would authorize all executive agencies to (1) exclude a source that fails to meet certain qualification requirements intended to reduce supply chain risk in the acquisition of IT; (2) exclude a source that fails to achieve an acceptable rating with regard to an evaluation factor providing for the consideration of supply chain risk in the evaluation of proposals for the award of a contract or the issuance of a task or delivery order; and (3) withhold consent for a contractor to subcontract with a particular source or direct a contractor to exclude a particular source from consideration for a subcontract under the prime contract. The executive agency would also be able to limit, in whole or in part, the disclosure of information relating to the basis for carrying out one of the aforementioned procurement actions. Importantly, if an executive agency has exercised its authority to limit disclosure of information, "no procurement action undertaken by the head of the agency under such authority shall be subject to review in a bid protest before the Government Accountability Office or in any Federal Court."

FASCA was read twice and referred to the Senate Committee on Homeland Security and Governmental Affairs on June 19, 2018. No further action has been taken.

Federal Information Technology Supply Chain Risk Management Improvement Act of 2018

On July 10, 2018, the Trump administration sent a legislative proposal for the Federal Information Technology Supply Chain Risk Management Improvement Act of 2018 to

continued on page 11

Congress. The proposal is similar to FASCA. In a press release, Senator McCaskill's office stated that "[b]oth McCaskill's bill [FASCA] and the Administration's language use similar methods to require greater accountability and increase transparency in the information technology acquisition process."

Like FASCA, the Federal Information Technology Supply Chain Risk Management Improvement Act proposes to establish a Federal Information Technology Acquisition Security Council as well as a Critical Information Technology Supply Chain Risk Evaluation Board, with many of the same member agencies as those identified in FASCA. The responsibilities of the Council would include, among others, identifying and recommending supply chain risk management standards for use by executive branch agencies and identifying criteria for sharing information with respect to supply chain risk. The responsibilities of the Board would include establishing criteria for recommending the exclusion of sources from executive agency procurements.

The Federal Information Technology Supply Chain Risk Management Improvement Act would also authorize executive agencies to take certain procurement actions to keep supply chain risks at bay. In addition to those procurement actions authorized by FASCA (i.e., excluding sources that fail to meet certain qualifications or ratings and withholding consent for subcontractors), the Federal Information Technology Supply Chain Risk Management Improvement Act would authorize executive agencies to determine that a contractor is not responsible based on supply chain risk considerations.

Recommendations for Contractors

Considering the similarities between the two legislative proposals, the trend is clear: the White House and Congress are interested in mitigating IT and supply chain risks through inter-agency councils and increased civilian agency authority to make procurement decisions (including source exclusions) based on supply chain risk. Although neither legislative proposal poses imminent change, the trend is clear. In the meantime, it will be important for contractors to anticipate these changes and shore up their IT and supply chain posture and ensure that key supply chain partners will withstand additional scrutiny. Contractors should also seek opportunities for engagement in shaping the implementation of these new trends. For example, one of the functions of the proposed Federal Acquisition Security Council would be to consult, as appropriate, with the private sector and other nongovernmental stakeholders on issues relating to the management of supply chain risks posed by the acquisition of IT.

For more information, please contact:

Nina S. Samuels
202.719.3761
nsamuels@wileyrein.com

CFIUS Reform Legislation Signed into Law with New Mandatory Reporting Requirements

By Daniel P. Brooks

The Committee on Foreign Investment in the United States (CFIUS) reviews foreign acquisitions of U.S. companies for national security considerations. Its rulings have significant impacts on U.S. investment policy and foreign investment flows into the U.S., especially those from China. On August 13, 2018, the President signed the Foreign Investment Risk Review Modernization Act (FIRRMA) into law as part of the FY 2019 NDAA.

FIRRMA significantly expands the jurisdiction and operational mandate of CFIUS to review transactions that were not previously subject to CFIUS scrutiny and reforms the CFIUS review process in several other important respects, including the addition of new mandatory reporting requirements. Although the CFIUS process has traditionally been voluntary, certain investment reporting will now be mandatory, with failure to report subject to civil penalty. The following is a summary of some of the law's major provisions.

Expanded Scope of Transactions Subject to CFIUS Jurisdiction

Whereas CFIUS was previously authorized to review only transactions that could result in foreign control of a U.S. business, ***CFIUS will now be able to review certain non-controlling investments***. These include non-controlling investments in businesses dealing with critical technologies, critical infrastructure, and sensitive personal data of U.S. citizens if the investment could provide the foreign person access to material nonpublic technical information, board membership or observer rights or the right to nominate a board member, or certain substantive decision-making involvement (other than through voting of shares). Investments by a foreign person through an investment fund that affords the foreign person membership as a limited partner on an advisory board or committee of the fund will be excluded from these new provisions, provided certain criteria are met.

FIRRMA also authorizes CFIUS to review transactions involving the purchase or lease of private or public real estate located within the United States, if it is located within an air or maritime port or in close proximity to a U.S. military installation or another sensitive U.S. Government facility. The purchase or lease of a single housing unit or real estate in an urbanized area will generally not be treated as a covered transaction, though CFIUS is authorized to prescribe regulations limiting this exception. FIRRMA also treats as a covered transaction any change in the rights that a foreign person has with respect to a U.S. business in which the foreign person has an investment if the change could result in foreign control of the U.S. business or an investment in a critical technology company, a critical infrastructure company, or a company that maintains or collects sensitive personal data of U.S. citizens as described above.

Voluntary and Mandatory Declarations

FIRRMA allows parties to a covered transaction to submit short-form "declarations" in lieu of a written notice. Such "short-form" filings will provide basic information regarding the transaction and generally will not exceed five pages in length. Within 30 days of the submission of a declaration, CFIUS will either (1) request that the parties file a written notice; (2) inform the parties that it is unable to complete action with respect to the transaction on the basis of the declaration alone; (3)

continued on page 13

initiate a unilateral review of the transaction; or (4) notify the parties in writing that the Committee has completed all action with respect to the transaction.

Subject to certain exceptions, declarations will be mandatory for any transaction involving the direct or indirect acquisition of a substantial interest in a critical technology company, a critical infrastructure company, or a company that maintains or collects sensitive personal data of U.S. citizens by a foreign person in which a foreign government has a direct or indirect substantial interest. The term "substantial interest" will be defined in the implementing regulations but will not include voting interests of ten percent or less. FIRRMA also authorizes CFIUS to require the submission of declarations for covered transactions involving critical technology companies.

Enhanced Mitigation Provisions

FIRRMA allows CFIUS to enter into and impose mitigation agreements and conditions in cases where a party to a covered transaction has voluntarily chosen to abandon the transaction and to enter into and impose mitigation agreements and conditions on covered transactions that have already been completed. FIRRMA prohibits CFIUS from entering into any mitigation agreement or imposing any condition unless CFIUS determines that the agreement or condition resolves the national security concerns and requires CFIUS to formulate plans for monitoring parties' compliance.

Other Notable Provisions

In addition to the changes noted above, FIRRMA also lengthens the initial CFIUS review period from 30 days to 45 days; allows CFIUS to extend an investigation for one 15-day period in "extraordinary circumstances"; permits and encourages the disclosure of confidential information to local and allied foreign governments for national security purposes; allows CFIUS to suspend a proposed or pending covered transaction while the transaction is under review; and authorizes CFIUS to collect a filing fee capped at the lesser of $300,000 or one percent of the value of the transaction.

Implementation and Next Steps

While many provisions of FIRRMA become effective immediately, other provisions (including those expanding the scope of what constitutes a "covered transaction" and provisions governing voluntary and mandatory declarations) will not go into effect until the earlier of 18 months after enactment or 30 days after publication in the *Federal Register* of a determination by CFIUS that the regulations, organizational structure, personnel, and other resources necessary to administer the law's provisions are in place. The focus now turns to the rulemaking process, where stakeholders will have an opportunity to submit comments and help shape the regulations that the U.S. Department of Treasury ultimately adopts to implement this sweeping new law. We also expect CFIUS to launch one or more pilot programs in the coming months to implement certain new authorities under FIRRMA. The scope and procedures for any pilot programs under FIRRMA will be published in the *Federal Register* in advance.

For more information, please contact:

Daniel P. Brooks
202.719.4183
dbrooks@wileyrein.com

Protect Your Company from the Unexpected: Preparing for and Responding to a Search Warrant Raid

By Kevin B. Muhlendorf and Michelle B. Bradshaw

Training for emergencies that require immediate and coordinated responses should be second-nature. When you board a plane, you know what to do in the unlikely event of a crash landing; if there is a fire, you know where to find the fire exit and rally point. Preparation for the execution of a search warrant is just as critical for your company, yet most businesses never train to handle this emergency. In failing to plan for the unthinkable, companies risk missing key opportunities to minimize liability, improve legal defenses, and maintain uninterrupted business operations.

Search Warrant Primer

A search warrant is a court order authorizing law enforcement to search a particular location and seize particular categories of things. It is issued by a judicial officer after a finding of probable cause—meaning there is a reasonable basis to believe that a crime has been committed and that evidence of that crime will be found at the location to be searched. Search warrants are executed by law enforcement without any notice to the target or time to prepare a response. Execution of a search warrant is often a company's first indication that it is the subject or target of a criminal investigation. Alternatively, the Government may believe the company merely possesses evidence of criminal conduct by some other individual or entity.

Below are steps companies should take proactively to minimize corporate risk in the event of a search warrant. Experienced counsel can tailor these plans to your business to best protect both your company and its employees.

Preparing for a Search Warrant Raid

- **Establish Appropriate Procedures.** Develop a search warrant response protocol consistent with this guidance. Consult with experienced white-collar counsel to tailor this plan to your company's size, scope, and particular needs.
- **Identify Key Company Personnel**. Form a search warrant response team at each facility. Designate a response team leader. This should be either a senior manager or corporate compliance officer. This leader and other appropriate company officials should be responsible for coordinating a response to a search warrant.
- **Identify Privileged Information**. Privileged documents should be segregated and clearly marked as "privileged" *before* a search warrant is executed to reduce the odds of inadvertent seizure. Prepare and maintain a list of in-house and outside counsel whose communications might fall under attorney-client privilege.
- **Duplicate Records.** Maintain a copy of essential business records at an off-site location. Periodically update this set of records. Agents will seize original business records and the company may not receive copies of seized records during the investigation.

continued on page 15

Managing Logistics During a Search Warrant Raid

You should educate your search warrant response team on the following procedures:

- **Call Response Team Leader**. Agents' first contact is often a receptionist or security officer at the entrance to the facility/office. This individual should *politely* (1) advise the agent that they do not have authority to accept legal process on behalf of the company; (2) request permission to contact someone with this authority before the agents continue; and (3) immediately notify the response team leader that agents are on the premises with a search warrant and the response team should assemble immediately.
- **Call Outside Counsel**. The response team leader should immediately contact outside counsel. Contact information for Wiley Rein White Collar Defense & Government Investigations attorneys is listed below. Notify your counsel as soon as agents arrive with a search warrant and speak to the Government only through your counsel.
- **Control Information Flow**. Tell the Government that it is company policy to cooperate with the search and that all questions should be directed to the designated response team leader. Upon arrival, outside counsel should serve as the main liaison with the agents, prosecutors, and issuing court.
- **Negotiate Reasonable Procedures**. Ask the agents to hold off the search for a brief period until outside counsel arrives. If this request is not honored, request that the agents participate in a pre-search telephone conference with outside counsel. If the agents refuse, seek to negotiate some ground rules for the search, including making copies of seized documents, computer data, and crucial business information such as personnel records, payables, receivables, customer lists, sales information, and billing records.
- **Gather Basic Information**. Obtain copies of search warrants (and all attachments), supporting affidavits, and subpoenas. If you are not permitted to review a document, ask why it is not being provided to you. Ask for business cards from all agents on the premises. This is an easy way to record the identity of all agents involved in the search and their respective agencies. Ask questions about the purpose of the search, the nature of the investigation, whether the company is a target, whether any employee is a target, and so on.
- **Review the Search Warrant Carefully**. The search warrant will describe the premises and establish parameters for the authorized search. Confirm the premises description includes your address (in the unlikely event agents have the incorrect address). Identify time limitations for the execution of the search and the specific areas the agents are authorized to enter. The warrant may not necessarily provide the agents access to all parts of the facility. If it does not, then the agents should be confined to only the specified areas. If the agents insist on entering areas not specified in the warrant, then the response team leader should *politely* object. Although this may not prevent entry, it will eliminate the Government's ability to later argue that consent was given to expand the search. Take detailed notes or photographs of the agent's conduct.

continued on page 16

- **Protect Privileged Materials**. Generally, search warrants do not authorize the seizure of privileged materials. Alert the agents regarding privileged documents on site. Request that these materials not be reviewed or taken. If they are taken, ask that they be sealed. Be sure to note an objection if the agents fail to comply with these requests.
- **Document Communications and Search Activities**. Ask to accompany the agents to direct them to areas described in the warrant. Take extensive notes regarding places searched, employees questioned, questions asked, statements made, time involved in each part of the search, and so on. Questions about certain items' locations contain valuable information about the Government's sources of information and possible investigative focus. The agents are not required to allow you to accompany them.
- **Utilize IT Personnel**. Search warrants invariably require the production of computer records. If possible, company IT personnel should ensure that the search does not extend beyond permissible areas and should facilitate the imaging of computers and peripherals so that they remain available for the ongoing operations of the business.
- **Manage Employees**. Gather all non-essential employees in a central location separate from the search. Inform them of their rights and obligations, set forth in the attached Employee Advice Checklist. After educating employees, send all non-essential employees home. Otherwise, agents will likely seek to interview key employees during the search. If the agents request to interview employees, respond that you would like to discuss the issue with counsel. If agents proceed with interviews, request that outside counsel be present.
- **Maintain Your Own Inventory**. As agents search the premises, maintain a detailed inventory of the materials seized. List box numbers for crucial documents. Request that a copy be made on the premises of all documents seized.
- **Obtain the Agents' Inventory**. You are entitled to a complete and accurate inventory of all items seized. Ask the agents to confirm that the inventory provided is a complete list of everything seized. Do not sign a receipt for the inventory.
- **Cooperate**. Be courteous, cooperative, and quiet.

Actions to Avoid During a Search Warrant Raid

Do not interfere with the Government's investigation. Specifically, your company and employees:

- **Must Not Interfere with the Search**. Do not do anything that may be interpreted as obstruction. Do not destroy, modify, remove, or conceal records or other materials. Do not intentionally make false statements to any federal agent.
- **Must Not Volunteer Information**. Do not volunteer any information without appropriate company authorization informed by counsel's advice. Your employees do not have a legal obligation to submit to an interview by government agents. Neither the company nor your employees are required to authenticate documents seized or otherwise respond to any questions.

continued on page 17

- **Must Not Expand the Scope**. Sometimes, agents may ask for consent to expand the search beyond the scope the search warrant permits. Do not consent to additional searches that the warrant does not authorize without consulting counsel about potential consequences. The company has no obligation to consent to this expansion. It does not have to decide immediately whether to voluntarily produce documents to the Government. The company can always agree to cooperate and voluntarily provide requested documents after the search after consulting with counsel. Often, execution of the search warrant will be accompanied by service of a grand jury subpoena for documents. Counsel can work with the Government to negotiate the scope and timing of any additional productions.
- **Must Not Prohibit Employees from Speaking to Government Agents**. Inform employees of their rights and obligations, including the right not to speak with law enforcement, then send all non-essential employees home.
- **Should Not Consent to Voluntary Interviews Without Counsel**. Request that outside counsel be present during any employee interviews.
- **Must Not Waive Privilege**. Do not communicate about privileged matters in a way that may waive the privilege.

Employee Advice Checklist

1. Agents have a legal right to search the premises and seize evidence designated in the warrant.
2. Employees should not obstruct the search.
3. Employees have no legal obligation to participate in an interview with agents.
4. Anything employees say can be used against them in a criminal prosecution or civil enforcement proceeding regardless of whether agents warn them.
5. Only give truthful, non-misleading answers.
6. If employees grant interviews they have a right to have an attorney present.
7. The company requests employees notify the company's counsel before interviewing so that the company's counsel can be present.
8. If employees are questioned outside the company counsel's presence, employees have a right to tell the company about the substance of their interviews.
9. Company counsel represents the company, not its employees.

For more information, please contact:

Kevin B. Muhlendorf
202.719.7052
kmuhlendorf@wileyrein.com

Michelle B. Bradshaw
202.719.7290
mbradshaw@wileyrein.com

ISDC Report to Congress for FY17: Suspensions and Debarments Decrease, and More Agencies Use "Pre-Notice Letters"

By Kara M. Sacilotto

On July 31, 2018, the Interagency Suspension and Debarment Committee (ISDC), an interagency body created by Executive Order 12549 to provide support for suspension and debarment programs throughout the Government, released its annual **report** to Congress, pursuant to Section 873 of the FY 2009 NDAA, regarding suspension and debarment activities during FY17. The report identifies the activities the ISDC pursued in furtherance of its four strategic objectives: promoting fundamental fairness in the suspension/debarment process; increasing transparency; enhancing federal suspension and debarment practices; and encouraging the development of more effective compliance and ethics programs by contractors. These activities included providing member program training with an emphasis on procedural consistency, transparency, and fairness; inviting private stakeholders to make presentations to ISDC agencies; maintaining ISDC's website to increase transparency; and improving the effectiveness of ISDC operations.

The ISDC also reported on survey results from its participating agencies. Notably, in FY17, agency suspensions and debarments decreased 14 percent from FY16, with agencies reporting 604 suspensions, 1613 proposed debarments, and 1423 debarments in FY17. Although a decrease from FY16, the report notes that these figures represent nearly double the activity reported in FY09, when the ISDC began tracking this data. This decrease cannot be explained by statistics on proactive outreaches by contractors before a debarring official raises concerns, because the number of reported proactive engagements also decreased from 76 to 53 between FY16 and FY17. Nonetheless, as the report recognizes, these types of outreach are beneficial to both contractors and debarring officials because they allow both parties to focus on any remedial or corrective actions before an exclusion might be deemed necessary by a debarring official. In this report, DOD agencies and the Department of Housing and Urban Development, among civilian agencies, had the most exclusionary actions.

Perhaps tracking the reduced number of exclusions, the use of administrative agreements, which are used as an alternative to suspension and debarment, also decreased between FY16 and FY17. In FY16, 75 administrative agreements were reported in contrast to 64 agreements entered into by 14 agencies in FY17. Even this reduced number is significantly higher than the administrative agreements reported in FY09 (35 agreements by five agencies). Over the past five years, 17 agencies also reported having entered into administrative agreements with individuals.

The most encouraging statistic, however, relates to the use of "pre-notice letters," such as show cause letters or requests for information. From FY16 to FY17, the use of such pre-notice letters jumped 21 percent (from 160 to 193) and represent a nearly three-fold increase from FY09. This is good news for contractors. Pre-notice letters are not specifically identified as a tool or option in the FAR. Nonetheless, as the ISDC report notes "[u]se of these letters helps the agency better assess the risk to the Government's interests without immediately imposing an exclusion

continued on page 21

action," which is the effect of a suspension or proposed debarment under FAR subpart 9.4. The increased use of these "pre-notice letters" provide contractors an opportunity to address a debarring official's concerns with the same seriousness of purpose as an exclusion action, but maintain the ability to generate income, improve performance, and demonstrate responsibility real-time by working with the Government. Because the debilitating effects of an exclusion are not imposed, such letters also provide the time and opportunity to open and continue a dialog between the contractor and debarring official's office, which should help a contractor committed to demonstrating present responsibility avoid an exclusion down the road. The Department of the Navy, General Services Administration, and Environmental Protection Agency reported issuing the most pre-notice letters in FY17.

In other good news, the ISDC states that it is exploring means of promoting consistency between procurement and non-procurement suspension and debarment procedures. Noting that a notice of proposed debarment under the FAR leads to immediate exclusion whereas the same notice provided under the Non-Procurement Common Rule, 2 C.F.R. Part 180, does not, the ISDC reports that it is exploring standardizing practices between the procurement and non-procurement community. In particular, the report notes that the ISDC "is considering the benefits and drawbacks of utilizing the nonprocurement approach."

This is good news because exclusion under the FAR and the Non-Procurement Common Rule are reciprocal, meaning an exclusion under one is an exclusion under the other. Yet, there are two sets of rules with different exclusionary results and different factors a debarring official should consider when assessing present responsibility. These differences risk inconsistent application and results. Standardization and consistency also would benefit the suspension and debarment system by creating a single set of rules and factors to consider.

Overall, the ISDC's FY17 report shows that the ISDC's efforts to strength suspension and debarment practices, but also promote fairness and transparency, through training, outreach, and sharing of best practices are yielding results. After a period when many agencies had programs that either "did not exist or had significant weaknesses," and then perhaps a period of "over-correction" to increase statistics by excluding contractors outright that may not have presented an immediate risk to the Government's interests, debarment programs seem to be maturing and using more non-exclusionary ways of ensuring the contractors with whom they do business are presently responsible. Good news all around.

For more information, please contact:

Kara M. Sacilotto
202.719.7107
ksacilotto@wileyrein.com

Speeches & Publications

Current Enforcement Environment and Pitfalls for Federal Grantees
April 23-25, 2019 | Crystal City, VA
nVISION Grants Management, NGMA's 2019 Annual Grants Training
Brian Walsh, Kendra P. Norwood

ACI's 6th Annual Forum on False Claims & Qui Tam Enforcement
January 28-29, 2019 | New York, NY
Roderick L. Thomas

809 Panel Recommendations
December 6, 2018 | Washington, DC
Nash & Cibinic Report Roundtable
Paul F. Khoury

Bid Protest Panel
November 14, 2018 | Washington, DC
U.S. Court of Federal Claims Judicial Conference
Paul F. Khoury

Bid Protest Developments and Strategy
October 18, 2018 | Washington, DC
Federal Publications Year in Review Conference
Paul F. Khoury, Brian Walsh

What to Watch For: Key Risk Areas and Pitfalls for Federal Grantees
September 26, 2018 | Online Webinar
Thompson Information Services
Brian Walsh, Kendra P. Norwood

Government Contractors Forum: Mandatory Disclosures for Federal Government Contractors: What, How, and When?
September 25, 2018 | McLean, VA
ACC National Captial Region
Kevin B. Muhlendorf, Kara M. Sacilotto

Protest Processes at GAO and COFC
September 17-18, 2018 | Washington, DC
ABA Section of Public Contract Law Introduction to Government Contracts Course
Paul F. Khoury

Subcontracting Issues Panel
September 17-18, 2018 | Washington, DC
ABA Section of Public Contract Law Introduction to Government Contracts Course
Tracye Winfrey Howard

Introduction to Government Contracts
September 17-18, 2018 | Washington, DC
ABA Section of Public Contract Law Introduction to Government Contracts Course
Kara M. Sacilotto

Record Retention Requirements for Federal Government Contractors and Grant Recipients
September 11, 2018 | Online Webinar
Clear Law Institute
Eric W. Leonard

continued on page 24

Speeches & Publications *continued from page 23*

Complying With New Government Contract Security Requirements

August 29, 2018 | Online Webinar

Lorman Education Services

Eric W. Leonard

DOJ's New Policy on FCA Dismissals Highlights Circuit Split

August 20, 2018 | ARTICLE

Law360

Madeline J. Cohen, P. Nicholas Peterson

One is the Loneliest Number: A Case for Changing Suspension and Debarment Regulations to Better Address Potential Exclusion of Individuals

Summer 2018 | ARTICLE

ABA Section of Public Contract Law Journal

Kara M. Sacilotto

NDAA Webinar: Everything You Need to Know About the New National Defense Authorization Act

August 16, 2018 | Online Webinar

Nova J. Daly, Daniel B. Pickard, Megan L. Brown, Tracye Winfrey Howard

A U.S. Perspective on the Investigation and Prosecution of Business Crimes

August 7, 2018 | Washington, DC

International Law Institute: Effective Prosecution of Financial Crimes, Cyber Crime and Human Trafficking

Kevin B. Muhlendorf

A Look Inside the Little-Known World of Government Contracts Law

August 1, 2018 | New Orleans, LA

National Bar Association Annual Convention

Kendra P. Norwood

National Defense Authorization Act for Fiscal Year 2019 Includes Acquisition Reforms That Contractors Should Be Aware Of *continued from page 6*

the same or comparable products and (2) reducing the amount of cost and pricing data required for such purchases. No more than ten contracts may be part of the pilot program and none of the contracts may be for major defense acquisition programs. By January 30, 2021, DOD must report the results of the pilot program to Congress, including an assessment of whether it should be continued or expanded.

For more information, please contact:

Tracye Winfrey Howard
202.719.7452
twhoward@wileyrein.com

Kendra P. Norwood
202.719.7069
knorwood@wileyrein.com

GOVERNMENT CONTRACTS TEAM PARTNERS/OF COUNSEL

Paul F. Khoury, Co-Chair	202.719.7346	pkhoury@wileyrein.com
Scott M. McCaleb, Co-Chair	202.719.3193	smccaleb@wileyrein.com
Rachel A. Alexander	202.719.7371	ralexander@wileyrein.com
Rand L. Allen	202.719.7329	rallen@wileyrein.com
Attison L. Barnes, III	202.717.7385	abarnes@wileyrein.com
Todd A. Bromberg	202.717.7357	tbromberg@wileyrein.com
Megan L. Brown	202.719.7579	mbrown@wileyrein.com
Kathryn Bucher	202.719.7530	kbucher@wileyrein.com
Jon W. Burd	202.719.7172	jburd@wileyrein.com
Ralph J. Caccia	202.719.7242	rcaccia@wileyrein.com
Philip J. Davis	202.719.7044	pdavis@wileyrein.com
Scott A. Felder	202.719.7029	sfelder@wileyrein.com
Matthew J. Gardner	202.719.4108	mgardner@wileyrein.com
Tracye Winfrey Howard	202.719.7452	twhoward@wileyrein.com
Eric W. Leonard	202.719.7185	eleonard@wileyrein.com
Kevin J. Maynard	202.719.3143	kmaynard@wileyrein.com
Christopher M. Mills	202.719.4740	cmills@wileyrein.com
Kevin B. Muhlendorf	202.719.7052	kmuhlendorf@wileyrein.com
Richard B. O'Keeffe, Jr.	202.719.7396	rokeeffe@wileyrein.com
Stephen J. Obermeier	202.719.7465	sobermeier@wileyrein.com
Dorthula H. Powell-Woodson	202.719.7150	dpowell-woodson@wileyrein.com
John R. Prairie	202.719.7167	jprairie@wileyrein.com
William A. Roberts, III	202.719.4955	wroberts@wileyrein.com
Kara M. Sacilotto	202.719.7107	ksacilotto@wileyrein.com
John R. Shane	202.719.7222	jshane@wileyrein.com
Craig Smith	202.719.7297	csmith@wileyrein.com
Mark B. Sweet	202.719.4649	msweet@wileyrein.com
Kay Tatum	202.719.7368	ktatum@wileyrein.com
Roderick L. Thomas	202.719.7035	rthomas@wileyrein.com
Brian Walsh	202.719.7469	bwalsh@wileyrein.com
Tara L. Ward	202.719.7495	tward@wileyrein.com
Gregory M. Williams	202.719.7593	gwilliams@wileyrein.com

GOVERNMENT CONTRACTS TEAM ASSOCIATES

Lindy Bathurst	202.719.7287	lbathurst@wileyrein.com
Michelle B. Bradshaw	202.719.7290	mbradshaw@wileyrein.com
Moshe B. Broder	202.219.4186	mbroder@wileyrein.com
Katherine C. Campbell	202.719.7583	kcampbell@wileyrein.com
Colin J. Cloherty	202.719.3564	ccloherty@wileyrein.com
J. Ryan Frazee	202.719.3751	jfrazee@wileyrein.com
Sarah B. Hansen*	202.719.7294	shansen@wileyrein.com
Cara L. Lasley	202.719.4192	clasley@wileyrein.com
Samantha S. Lee	202.719.7551	sslee@wileyrein.com
Kendra P. Norwood	202.719.7069	knorwood@wileyrein.com
George E. Petel	202.719.3759	gpetel@wileyrein.com
Nina S. Samuels	202.719.3761	nsamuels@wileyrein.com
Gary S. Ward	202.719.7571	gsward@wileyrein.com

To update your contact information or to cancel your subscription to this newsletter, visit:

www.wileyrein.com/newsroom-signup.html.

*District of Columbia Bar pending, supervised by principals of the firm