Wiley Rein LLP

GOVERNMENT CONTRACTS ISSUE UPDATE

November 2017

DCMA Improves Guidance for Purchasing System Reviews

By Tracye Winfrey Howard and Craig Smith

Earlier this month, the Defense Contract Management Agency (DCMA) issued its latest update to the ***Contractor Purchasing System Review (CPSR) Guidebook***. The Guidebook is intended to provide guidance and procedures to government personnel for evaluating contractor purchasing systems and preparing CPSR reports. These updates help fill important gaps in DCMA purchasing system guidance, but other ambiguities remain.

What is the CPSR Guidebook?

Large defense contractors often have a requirement for their purchasing and similar business systems that other contractors and businesses do not: satisfying obligations imposed by the Department of Defense (DOD) business-systems rules. For purchasing systems, DCMA assesses compliance with those obligations through CPSRs. DCMA has long published the

continued on page 2

ALSO IN THIS ISSUE

As Deadline for Contractor Cybersecurity Compliance Looms, DOD Acknowledges Industry Gaps

By Jon W. Burd and Matthew J. Gardner

As the December 31, 2017 deadline approaches for contractors to implement NIST SP 800-171 cybersecurity requirements outlined in DFARS clause 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting), ***DOD recently issued guidance*** tacitly acknowledging that industry is not fully prepared to be compliant by the deadline, and outlining the process DOD will use to "transition" to full compliance. This update highlights important steps for contractors who are still working to become NIST SP 800-171 compliant.

continued on page 3

DCMA Improves Guidance for Purchasing System Reviews

continued from page 1

CPSR Guidebook to both standardize and explain how it assesses compliance with the DOD purchasing systems requirements. The Guidebook serves as a roadmap not only for DCMA's CPSR Group and Administrative Contracting Officers who conduct and assess the CPSRs, but also for contractors to build and tailor their purchasing systems and prepare them for CPSRs. Over the past two years, DCMA issued rolling updates to expand the Guidebook's discussion of substantive assessments; the most recent updates were issued on October 2, 2017.

Guidebook Expansions Clarify Practices

Experience suggests the latest CPSR Guidebook updates will be positive developments for covered contractors because they reduce some of the mystery, if not the burden, of maintaining a DOD-compliant purchasing system. Collectively, the Guidebook expansions comprise 30 appendices covering the topical areas that DCMA reviews during CPSRs. Each appendix cites the relevant statutory and regulatory obligations, followed by DCMA's criteria for compliant policies and "practices."

These policy and practice reviews are at the heart of each CPSR, and the Guidebook updates fill a major gap in prior versions, which listed the topical areas DCMA reviews but did not describe how DCMA assessed compliance in those areas. CPSR results often surprised contractors under the old Guidebook because DCMA imposed compliance obligations not found in the text of the relevant statutes and regulations. Now, with the updated Guidebook, contractors are at least on notice of DCMA's interpretive positions and can prepare their purchasing systems accordingly.

The most recent Guidebook update also includes updated appendices covering requirements for negotiating with subcontractors, documenting compliance with purchasing obligations, counterfeit parts mitigation and surveillance, and a broad class of domestic-preference requirements under the "Buy American" umbrella.

Supply-chain professionals in large defense contractors should consider these appendices valuable tools for developing purchasing system policies and procedures, as well preparing for CPSRs. At a minimum, they should be consulted as a baseline for updating policies and revising workflows. They also provide an objective measure for testing the system by outside professionals familiar with CPSRs.

No Path to Perfection

Of course, mock audits based on the updated Guidebook appendices will also highlight some of the CPSR Guidebook's continued limitations. Even after the most recent updates, the scope and boundary of some areas of DCMA's review can be hard to discern. For example, the new "Buy American" appendix (#25) broadly discusses not just the Buy American Act, but also the Berry Amendment, Executive Order 13788 (Buy American, Hire American), and other topics. Yet under the headers for compliant policies and practices, the Guidebook focuses mostly on flowdown of FAR and DFARS clauses and on reporting required by DFARS 252.225-7004, Report of Intended Performance Outside of the United States and Canada. These disconnects contribute to ambiguity in how DCMA will assess "Buy American" compliance (narrowly or broadly) in a CPSR.

continued on page 3

DCMA Improves Guidance for Purchasing System Reviews

continued from page 2

The updated Guidebook also failed to correct other shortcomings in predecessor versions. For example, Appendix 21 covers a contractor's commercial-item *determinations*. But the appendix includes directions to check during a CPSR that the contractor has documented price reasonableness analyses to support its commercial-item determinations. Price *reasonableness* is, of course, a separate assessment that is often (improperly) conflated with a determination of whether a product or service meets the criteria for a commercial item. Earlier this year, DOD confirmed the distinction through draft updates to its Commercial Item Guidebook. In contrast, DCMA's CPSR Guidebook continues to conflate the two concepts/analyses, at least in part—a practice that experience suggests is consistent with the view of DCMA auditors. Setting aside disagreement about the policy and approach, however, the updated Guidebook appendices at least forewarn contractors on how they should anticipate and prepare for CPSR audits until the Guidebook is further refined.

Overall, these appendices updating CPSR practices are positive additions to the CPSR Guidebook. We have found the appendices helpful in preparing for CPSRs and responding to CPSR audit reports. We recommend that contractors review these documents, then consult within and outside their supply-chain organization to assess how ready their purchasing system is for the next DCMA review. ■

For more information, please contact:

Tracye Winfrey Howard
202.719.7452
twhoward@wileyrein.com

Craig Smith
202.719.7297
csmith@wileyrein.com

As Deadline for Contractor Cybersecurity Compliance Looms, DOD Acknowledges Industry Gaps

continued from page 1

The December 31, 2017 Deadline for NIST SP 800-171 Compliance

In August 2015, DOD issued an interim rule requiring defense contractors who have sensitive defense information residing on or transiting across their information systems to immediately implement the cybersecurity processes and protocols outlined in NIST SP 800-171. Following backlash from industry regarding the time and resources needed to comply with these requirements, in December 2015 DOD revised DFARS clause 252.204-7012 to include a two-year grace period for contractors to phase in NIST SP 800-171 compliant procedures.

Since then, the clause has required covered contractors to "implement NIST SP 800-171, ***as soon as practical***, but ***not later than December 31, 2017***." In the interim, contractors who did not yet fully comply with NIST SP 800-171 were required to "notify the DOD Chief Information Officer . . . within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award." Likewise, DFARS clause 252.204-7008 (Compliance with Safeguarding Covered Defense Information Controls) states that by submitting an offer, "the Offeror

continued on page 4

represents that it will implement the security requirements specified by [NIST SP 800-171] . . . ***not later than December 31, 2017.***"

This scheme established a requirement for contractors to either comply with NIST SP 800-171, or devote best efforts to establishing compliance by the end of 2017. While the two-year grace period seemed generous at first, anecdotal evidence suggests that the majority of covered contractors will not meet the December deadline and need more time. In theory, this could create a situation in which many contractors would be in breach of DFARS clause 252.204-7012 after the ball drop ushers in New Year's Day.

System Security Plans and Plans of Actions and Milestones Can Smooth Out Compliance Gaps

For covered contractors who do not expect to comply fully with NIST SP 800-171 requirements by the deadline, a recent update provides measured relief. In December 2016, NIST issued SP 800-171 "Revision 1," which updated guidance on the use of system security plans (SSPs) and plans of action and milestones (POAMs) to document gaps in an organization's security posture and the actions the contractor plans to take to overcome them:

> Nonfederal organizations should describe in a system security plan, how the specified security requirements are met or how organizations plan to meet the requirements. The plan describes the system boundary; the operational environment; how the security requirements are implemented; and the relationships with or connections to other systems. Nonfederal organizations should develop plans of action that ***describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented.***

NIST SP 800-171, Rev. 1 at 9. The update instructed contractors to use the SSP "to describe any enduring exceptions to the security requirements," while "***[i]ndividual, isolated, or temporary deficiencies should be managed through [POAMs]***."

At least in theory, a contractor can meet the contractual obligation to comply with NIST SP 800-171 by either fully implementing the procedures and protocols it requires, or by documenting potential gaps in the contractor's SSP and outlining the contractor's "get well" plan in the POAM.

DOD's Updated Guidance for Implementing the Security Requirements of NIST SP 800-171

In a September 19, 2017 Memorandum addressing "Implementation of DFARS Clause 252.204-7012," Shay Assad (Director, DPAP) issued guidance to DOD acquisition professionals that acknowledges—if not expressly states—that contractors may not have NIST SP 800-171 compliant systems by DOD's December 31, 2017 deadline. In a section on "Documenting a Contractor's Implementation or Planned Implementation of NIST 800-171," the Memorandum calls out the short-term flexibility that may be gained from SSPs and POAMs that identify and provide a plan for overcoming compliance gaps:

> To document implementation of the NIST SP 800-171 security requirements by the December 31, 2017 implementation deadline, companies should have a system security plan in place, ***in***

continued on page 5

> ***addition to any association plans of action to describe how and when any unimplemented security requirements will be met, how any planned mitigations will be implemented, and how and when they will correct deficiencies and reduce or eliminate vulnerabilities in the systems.***

The Memorandum identified different methods that contractors have for informing the Government of the contractor's implementation of NIST SP 800-171 requirements, including gaps outlined in the SSPs and POAMs. For contracts issued prior to October 1, 2017, contractors still have an affirmative obligation to identify gaps to the DOD CIO. In other cases, the Memorandum notes "the solicitation may require or allow elements of the system security plan, which demonstrates/documents implementation of NIST SP 800-171, to be included with the contractor's technical proposal, and may subsequently be incorporated (usually by reference) as part of the contract." Contractors should view such disclosures to the Government as a best practice if information systems are not fully compliant with NIST SP 800-171, in order to avoid allegations in hindsight that the contractor failed to meet contract requirements outlined in DFARS clause 252.204-712, or made a material misrepresentation of compliance under DFARS clause 252.204-7008.

But contractors should also be aware that NIST SP 800-171 compliance could quickly become a competitive discriminator, especially for programs that will require access to sensitive covered defense information. The Memorandum highlighted the potential role of SSPs and POAMs in the source selection process, and noted that "the requiring activity is not precluded from using a company's [SSPs and POAMs] to evaluate the overall risk introduced by the state of the contractor's internal information system/network." Requiring activities are likely to develop "safeguarding requirements for a given procurement and the level of risk they are willing to accept as industry transitions to full compliance of the NIST SP 800-171 security requirements," and make case-by-case determinations about how they plan to evaluate compliance risk in individual competitions. In some cases, an agency may determine that it requires ***all*** security requirements in NIST SP 800-171 to be met for an offeror to successfully compete. In others, the agency may "determine whether to accept the risk of storing sensitive government data on a contractor system that has not fully met the NIST SP 800-171 requirements," and opt to incorporate the successful offeror's SSP and POAM into the contract "to ensure the contractor is held accountable to meet the NIST SP 800-171 requirements in accordance with its own plans." ■

Wiley Rein remains active in this area and has advised clients on the scope of DFARS clause 252.204-7012, the implementation of NIST SP 800-171 requirements, and compliance with cyber incident reporting obligations. If you have questions about any of these issues, please contact:

Jon W. Burd
202.719.7172
jburd@wileyrein.com

Matthew J. Gardner
202.719.4108
mgardner@wileyrein.com

Frustration with Delays in DCAA Assist Audits for Subcontractor Cost and Pricing Data Prompts Outside the Box Solutions

By Tracye Winfrey Howard and George E. Petel

Audit delays are a constant source of frustration for the entire government contracts community – within both private industry and the Government. Although the Defense Contract Audit Agency (DCAA) has had some success in recent years winnowing its enormous backlog, audits can still take years to complete, substantially delaying contract close-outs. Delays in price proposal audits lead to delays in contract price negotiations, award, and eventual performance. The frustration with these delays has prompted congressional oversight and legislation, as well as counter-responses from DCAA.

DCAA's September 2017 Guidance

One such counter-response from DCAA is a September 2017 Memorandum for Regional Directors (MRD), titled "Audit Alert on Requirement for Prime Contractor Cost and Price Analysis." In this MRD, DCAA issued guidance meant to address questions related to price proposal audits, particularly situations where DCAA is asked to assist the contracting officer in establishing the reasonableness of proposed subcontractor prices. These price proposal audits generally arise on sole source awards or modifications to existing contracts, where lengthy price negotiations between the contractor and contracting officer are necessary.

The MRD advises DCAA auditors not to delay auditing subcontractor proposed prices, even if the prime contractor's own analysis of the subcontractor's prices is not yet complete. This approach is intended to mitigate delays in audits of the prime contractor's proposed price to the Government by having DCAA proceed based on all available information rather than waiting until the prime contractor has assembled its complete price proposal. The MRD emphasizes early engagement by DCAA with the contracting officer and the prime contractor to facilitate price proposal audits in the most efficient manner possible.

The MRD is presented in a question-and-answer format, which answers questions such as:

- Can DCAA audit a subcontract proposal prior to the prime contractor's submission of its management-approved proposal?
- Does an audit of a subcontract proposal relieve the prime contractor from its responsibility to perform cost or price analyses of the subcontract proposal?
- If the DCAA team auditing the prime contract proposal has requested a DCAA assist audit of a subcontract proposal, but the prime contractor has NOT performed the FAR 15.404-3(b)-required cost or price analyses to establish the reasonableness of the proposed subcontract price before DCAA completes its fieldwork on the prime contract proposal, should the prime audit team classify the proposed subcontract costs as unresolved or unsupported?

Per FAR 15.404-3(b), prime contractors or subcontractors must establish the reasonableness of subcontractor prices, and must provide support for the cost or price analyses in their proposals. Often, however, proposal deadlines make it impossible for prime contractors to complete the required analyses of their subcontractors' proposals

continued on page 7

before submission of the prime contract proposal, especially if the prime does not yet have full price proposals from its subcontractors. Instead, prime contractors will often include with their proposal a timeline for the receipt of subcontractor proposals, and work to complete the required analysis post-submission. Even if prime contractors do not have access to subcontractor cost data, the MRD makes clear that FAR 15.404-3 still requires some level of price analysis. The MRD puts the onus on the prime contractor to seek help from the contracting officer and to document its efforts to obtain the relevant data.

In the past, DCAA has refused to conduct any portion of the audit until the prime contactor's analysis of the subcontractor proposal is completed, merely finding the entire proposal "inadequate." The MRD ends that practice and states that contracting officers may request an audit of subcontractor proposals even before the prime contractor has completed its analysis, but that DCAA should mark the prime contractor's proposal as including inadequate cost or pricing data. As a result, DCAA auditors should now accept and begin work on prime contract audit engagements rather than refuse to audit an entire proposal submission based on the prime contractor's failure to include its analysis of subcontractor prices.

Practicalities and Potential Solutions

Despite this guidance, prime contractors should still ensure that their purchasing systems and personnel are up-to-date and equipped to handle the required analyses quickly and efficiently, whether that is a more limited price analysis or a complex cost analysis. Under the MRD, there is now a risk that if DCAA finishes its fieldwork before the prime contractor completes its review of the subcontractor proposal, DCAA will find the subcontractor proposal "unsupported" rather than merely "unresolved," indicating that DCAA's assist audit report has not been received.

This guidance was prompted, in part, by Congress's recent expressions of dissatisfaction (on behalf of contractor constituents) with delays in DCAA's assist audits. For example, in Section 820 of the National Defense Authorization Act (NDAA) for Fiscal Year 2017 (Pub. L. No. 114-328), Congress authorized outside audits of indirect costs under certain circumstances. Specifically, defense contractors may present their outside auditors' indirect cost findings to DCAA – and avoid any additional DCAA audit – as long as the auditors performed the audit in accordance with Generally Accepted Auditor Principles (GAAP) standards. Additionally, this past summer, the House Armed Services Committee's proposed acquisition reform bill included a provision that would revise the Fiscal Year 2017 NDAA provision to broaden acceptance of private audits even further by allowing Pentagon officials greater authority to circumvent DCAA and select a private auditor to perform incurred cost audits. Although some within and without the Government strongly object to the transfer of these services, which some view as "inherently governmental functions," to private parties, expansion of the role outside auditors play in government contracts is likely inevitable given DCAA's persistent, significant backlogs and their potential effects on the DOD mission.

continued on page 11

Congress Looks to Government Contractors to Fix IoT Cybersecurity, Raising Concerns

By Megan L. Brown, Matthew J. Gardner, and Moshe B. Broder

The Internet of Things (IoT) Cybersecurity Improvement Act of 2017, S.1691, introduced August 1, 2017, by Sens. Mark Warner (D-VA), Cory Gardner (R-CO), Ron Wyden (D-OR), and Steve Daines (R-MT), seeks to improve the security of IoT devices by establishing requirements for IoT devices procured by the federal government. Members of the house are working on a companion bill to S. 1691. Several congressional ***hearings*** have been held about IoT security, and ***efforts*** are underway throughout the executive branch. The private sector is likewise addressing IoT security, as explained in a ***recent paper by the U.S. Chamber of Commerce.***

The proposed law is designed to combat poor cybersecurity in IoT devices sold to the Government; however, securing surveillance cameras, traffic lights, autonomous cars, and similar remote sensors is not the end goal. Rather, drafters of the proposed law hope to prevent Distributed Denial of Service (DDoS) attacks that capitalize on the poor cybersecurity of some IoT devices and jeopardize life on the Internet.

The law, if enacted, would have significant impacts for contractors. Among other things, it would require companies selling connected products to the Government to make commitments about product security and expand support. The certifications about security could open the door to contractual and enforcement liability for noncompliance. The law would encourage more research and "hacking" of products provided to the Government, increasing burdens on those dealing with the federal government and depriving them of choice in whether and how to manage vulnerability disclosure.

As the Government looks at how to manage an increasingly dynamic technology landscape, those selling connected products to the Government should watch this and related developments.

Background on IoT Cybersecurity

Vulnerabilities in IoT devices are attracting increased attention as the number of IoT devices in use has expanded exponentially. The emerging consensus among security experts both in the private sector and Government is that IoT cybersecurity is often poor and presents a growing threat.

IoT devices are often built to be plugged in and forgotten about, and security is not given much (if any) attention. The security shortcomings are attributable to a number of factors unique to IoT products. IoT devices often have rudimentary operating systems, making advanced security features difficult to implement. Many devices are not protected by a firewall or router and are connected directly to the Internet. These devices are generally not patched or updated. Perhaps most alarming, many devices are shipped with default usernames and passwords built into the firmware, like "root" and "admin" or "test" and "1234."

This combination of default passwords, direct internet connections, and limited security precautions, makes IoT devices vulnerable. Hackers are able to scan random IP addresses for open connections and attempt a brute-force login with commonly-used or known default credentials. This method of attack is easy and effective.

continued on page 9

DDoS Attack on October 21, 2016

The proposed law is designed to help prevent the use of highly-vulnerable IoT devices to conduct large-scale DDoS attacks that are capable of shutting down portions of the Internet, like a significant and widespread DDoS attack on October 21, 2016. In general, DDoS attacks work by overwhelming a target with very high levels of traffic, causing the target to no longer respond to legitimate internet traffic. DDoS attacks are "distributed" because the attacker utilizes numerous IP addresses to launch the attack. Hackers often gain the needed computing power and diverse IP addresses needed to mount these attacks by hacking into numerous computers and forcing them to work in coordination. The hacked computers are referred to as a botnet. Because the attack comes from the large number of IP addresses that belong to the computers in the botnet, preventing a successful DDoS attack is not just a matter of denying internet traffic from a single malicious IP address.

The attack on October 21st followed this basic pattern. Unlike previous attacks, however, that DDoS attack utilized thousands of infected IoT devices, like video cameras with fixed administrator credentials, to create a massive botnet army. As a result, the attack was highly distributed and powerful, even compared to traditional DDoS attacks. The attack was focused on Dyn, a domain name server (DNS) lookup company that routes internet traffic and traditionally had very strong defenses. However, using the IoT devices, the botnet overwhelmed Dyn, which had a secondary effect of taking offline hundreds of websites, like Amazon, Etsy, and Twitter, that relied on Dyn. Security researchers fear that future DDoS attacks based on botnet armies of IoT devices could be powerful enough to constitute a significant threat to the Internet.

The Requirements Under the Proposed Law

To prevent future DDoS attacks that threaten the Internet, the proposed law aims to improve the cybersecurity of IoT devices sold to the Government, with the goal of reducing the threat of these devastating DDoS attacks. This may not come to fruition given the relatively small market share federal procurement has in the global market for connected devices. Nevertheless, putting aside efficacy of the legislation, there are some areas of practical concern as well.

For example, the proposed law would require contractors to make several certifications with respect to IoT devices, such as:

- The devices do not contain, at the time of proposal, any known "security vulnerabilities" in any hardware, software, or firmware component;
- The devices rely on components capable of accepting properly authenticated and trusted updates from the vendor;
- The devices use only "non-deprecated industry-standard protocols and technologies" for functions such as communications, encryption, and interconnection with other device or peripherals; and
- The devices do not include any fixed or hard-coded credentials or passwords used for remote administration, delivery of updates, or communication.

In addition, under the proposed law, companies that sell IoT devices to the Government will be required to create

continued on page 10

vulnerability disclosure programs. According to the proposed law, among other things, these programs will require the contractor to:

- Notify the purchasing agency of any known security vulnerabilities or defects subsequently disclosed to it or otherwise learned, for the duration of the contract;
- Update or replace any software or firmware;
- Timely repair any new security vulnerability, or replace the device, if an update does not remedy the issue; and
- Provide the purchasing agency with general information on the device to be updated, relating to the anticipated support and manner in which the device receives updates.

Are Burdens on Contractors the Right Remedy?

The certifications under the proposed law are designed to discourage the sale or use of IoT devices that can be easily hacked and used as part of a botnet army. Certainly, some changes may be relatively easy to implement. For example, eliminating fixed passwords like "1234" from the firmware of IoT devices would be a step in the right direction.

Nonetheless, the certifications appear likely to create compliance challenges for well-meaning contractors. There is ambiguity inherent in reporting known vulnerabilities and using industry standard protocols in a field as rapidly evolving as cybersecurity. Moreover, verifying, testing, and patching vulnerabilities is not always an easy process, putting contractors in a difficult position when the answer is more complex than a simple fix. Individuals who report vulnerabilities have mixed motives, and it is difficult for a company to quickly ascertain whether they are working with a genuine "white-hat" hacker with a legitimate bug or someone with a more nefarious agenda. It may be premature for the Government to mandate the use and particular design of vulnerability disclosure programs which are relatively new and with which the Government itself has little experience.

Correctly describing these inherently ambiguous situations to the Government will take on extra importance after the Supreme Court's decision in *Universal Health Services Inc. v. United States ex rel. Escobar*, 136 S. Ct. 1989 (2016), which held that contractors may be liable under the False Claims Act for "misleading half-truths" in certain situations. A good faith judgment call on reporting an uncertain vulnerability might look different when re-contextualized in the aftermath of a cyber incident.

Moreover, the scope of the bill is limited to government contractors. Even if government contractors are fully compliant and implement robust cybersecurity for IoT devices, will that eliminate the threat from DDoS attacks? That is unlikely. For example, it appears that video cameras sold by large Chinese electronics companies were a significant part of the botnet that was used in the DDoS attack in October 2016. The proposed bill would do nothing to directly change the behavior of the many companies selling IoT devices in the commercial market. As long as IoT devices with weak cybersecurity remain on the market, the possibility remains that hackers can exploit those devices to create DDoS attacks. This is why the ecosystem is taking layered steps to mitigate risks by, for example,

continued on page 11

Congress Looks to Government Contractors to Fix IoT Cybersecurity, Raising Concerns *continued from page 10*

filtering traffic and using third party security services to respond to DDoS attacks.

Other aspects of the draft legislation deserve careful consideration. Codifying technical definitions in the United States Code can make it hard to keep up with changing technology. Obsolescence is particularly a concern where those definitions will shape contract clauses that may linger for decades before the next revision. The legislation also calls for public lists of devices for which security support may have ceased and for which researchers have immunity to conduct research. This may worsen the security posture of federal networks.

Conclusion

Companies that make IoT devices for the Government should pay careful attention to this bipartisan legislation as it advances. The legislation has been hailed as a step in the right direction, but its complexity and unintended consequences should make technology companies think twice. While the threat posed by poor cybersecurity in IoT devices is daunting, it is not obvious that the proposed law would make material progress towards a solution. ■

For more information, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Matthew J. Gardner
202.719.4108
mgardner@wileyrein.com

Moshe B. Broder
202.719.7394
mbroder@wileyrein.com

Frustration with Delays in DCAA Assist Audits for Subcontractor Cost and Pricing Data Prompts Outside the Box Solutions *continued from page 7*

Conclusion

The new guidance from DCAA is unlikely to assuage contractor and congressional concerns with DCAA's audit delays. Nevertheless, the guidance is a welcome step, and should alleviate some of the burdens prime contractors currently face in getting price proposal audits completed in a timely manner. ■

For more information, please contact:

Tracye Winfrey Howard
202.719.7452
twhoward@wileyrein.com

George E. Petel
202.719.3759
gpetel@wileyrein.com

DOD Announces Acquisition Reorganization Efforts

By Richard B. O'Keeffe, Jr. and Lindy Bathurst

In early October, DOD and the Army announced renewed efforts to reorganize the defense acquisition workforce through the implementation of bureaucratic reforms and training initiatives.

Touted as some of the biggest reform efforts in the past decades, the Army and DOD are taking two distinct approaches to attempt to streamline the acquisition process, harness expertise, and renew focus on education and training. The major reform goals are: speeding up the acquisition process and tapping previously underused technical and operational expertise in drafting contract requirements.

However, whether these changes will have a real impact on procurement speed, efficiency and effectiveness, or whether it's just another round of personnel churn and reorganization, remains to be seen.

DOD Seeks Efficiency in Research & Development

As part of a Congressional mandate, DOD is in the process of reorganizing its workforce by splitting its Acquisition, Technology and Logistics (AT&L) section into two separate offices. In doing so, DOD must create two distinct branches of the acquisition workforce that will develop expertise within each new branch. The split, which is scheduled to go into effect February 2018, will result in a Research & Engineering Office, and an Acquisition & Sustainment Office.

The Research & Engineering (R&E) Branch will house technology development separately from the non-developmental installation and mission support acquisition processes. A new Under Secretary of Defense for Research and Engineering will oversee the branch with support from a newly created position, the Assistant Secretary of Defense for Acquisition Policy and Oversight. DOD will shift the Defense Advanced Research Projects Agency; the Strategic Capabilities Office; the Defense Threat Reduction Agency; the Missile Defense Agency; and the existing Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense under the new R&E Branch. DOD anticipates that by sectioning off R&E in a separate office, technology development will not be slowed by the acquisition lifecycle, and that the change will "[restore, elevate, and enhance] the mission of defense technological innovation."

The Acquisition & Sustainment Branch will manage acquisition policy and routine decision-making, and will be led by the Under Secretary of Management and Support.

In addition to the split, DOD is rolling out other initiatives with the goal of speeding the acquisition process. Specifically, DOD wants to cut contracting time in half. While this goal is certainly clear, the means to achieve it are not yet spelled out clearly, with simplification and utilization of new tools listed as the drivers for the desired change. More specifically, DOD is said to be considering greater use of Other Transaction Authority (OTA) by the new R&E Branch, which DOD hopes will enable more nimble acquisitions.

The Army Seeks Expertise in Developing Requirements

While DOD is splitting its acquisition function, the Army is planning to centralize its acquisition workforce by consolidating some of its larger contracting activities, including the Army Research & Development Command and the Army Capabilities Integration Center.

continued on page 13

Army officials are still working through details of the restructuring plan—their recommendations are due in February, and are expected to be implemented next summer. However, it is likely that the Army will look to units like the Army Rapid Capabilities Office (RCO)—created in August 2016 to provide equipment to select Army capabilities with a short turnaround time—as a model for implementing more efficient procurement processes.

Drawing on the RCO model, the Army wants to streamline the acquisition process by taking advantage of warfighter knowledge and cross-functionality, especially early in the procurement process. In an October 3 Memo entitled "Modernization Priorities for the United States Army," signed by Army Chief of Staff, Mark Milley, and Acting Secretary Ryan D. McCarthy, the Army noted its plan reduce the delivery time for new systems, and that it planned to use cross-functional teams, along with direct incorporation of warfighter knowledge during the Pre-Systems Acquisitions Stage.

These efforts were outlined in Army Directive 2017-24, which detailed the pilot program for the use of Cross-Functional Teams (CFTs). The CFTs will consist of personnel from different Army components, including Requirements, Acquisition Logisticians and U.S. Army Forces Command, and be tasked with writing contract requirements. The Army anticipates that use of CFT's will speed requirements development by pulling from multiple areas of expertise, incorporating end-user knowledge, and fostering a more iterative, rather than linear development process. The Army hopes another outcome will be clearer requirements that better match warfighter needs.

A Dual Focus on Education

Among both DOD's and the Army's reorganization efforts is a renewed focus on training and education in the acquisition workforce.

Part of the focus is hiring and retaining individuals with relevant with experience. The Army released Army Directive 2017-22, which focused in part on "Improving Talent Management," to "improve acquisition outcomes." Specifically, the Army wants acquisition personnel to have more operational experience.

Both DOD and the Army want to improve the training and educational opportunities available to the workforce. While the Army has not explicitly identified what type of training reforms will be implemented, Defense Undersecretary for Acquisition, Technology and Logistics Ellen Lord, has expressed the desire to update the content and offerings of the Defense Acquisition University (DAU), specifically in areas that have been highlighted as needing better oversight and management, such as service contracts.

What to Expect/What to Do

There is no doubt we have seen these initiatives before. The end state of a better trained, more stable acquisition workforce that can apply streamlined processes to provide faster and more responsive acquisition support to warfighters has been a goal that DOD has struggled to achieve for decades, with varying levels of success. For now, it is probably prudent for industry to assume that not much will change quickly, and to defer any business process changes based on the expectation that DOD will fundamentally alter its own business practices in the acquisition

continued on page 20

False Claims Act: *Escobar's* Materiality Language Gets More Bite

By Roderick L. Thomas and Michelle B. Bradshaw

For more than a year, courts have grappled with the Supreme Court's unanimous *Escobar* opinion, which altered the False Claims Act (FCA) landscape by reframing the "rigorous" nature of the FCA's materiality standard. See *Universal Health Servs., Inc. v. United States ex rel. Escobar*, 136 S. Ct. 1989 (2016). Since *Escobar*, courts have embraced this heightened materiality standard and affirmed dismissal where it is not satisfied.

The Supreme Court's Landmark *Escobar* Ruling

The *Escobar* opinion impacted FCA litigation in two significant ways. First, the Court upheld the implied false certification theory under certain circumstances. Second, the Court clarified that materiality is a "demanding" standard. To be actionable under the FCA, "[a] misrepresentation about compliance with a statutory, regulatory, or contractual requirement[s] must be *material* to the Government's payment decision." However, "[a] misrepresentation cannot be deemed material merely because the Government designates compliance with a particular statutory, regulatory, or contractual requirement as a condition of payment." The Government's actual knowledge of a violation of requirements, coupled with its payment of a particular claim in full, or regular payment of a particular type of claim in full without indicating an objection, "is strong evidence that the requirements [violated] are not material." The Court further explained that materiality is a proper basis for dismissing an FCA case on either a motion to dismiss or a motion for summary judgment.

Grappling with Post-*Escobar* Materiality

Since *Escobar*, courts have grappled with how to apply the announced standard. Defendants argue that *Escobar* raised the standard and imposed a greater burden on relators and the Government, focusing on the Court's discussion of the "rigorous" standard. Meanwhile, the Department of Justice has filed Statements of Interest in multiple cases arguing that *Escobar* did *not* change the materiality standard, focusing on the Court's discussion of statutory language and common law preceding its "demanding" standard discussion.

Several circuit court panels that have addressed the materiality standard in the wake of *Escobar* have embraced the heightened standard and focused on the impact of the government's knowing payment of claims notwithstanding some defect. They do not seem to have established a *per se* rule on government knowledge. In some cases, the plaintiff's attempt to demonstrate materiality failed where the Government investigated allegations or knowingly accepted the allegedly fraudulent information, but continued to authorize payment. *See, e.g., United States ex rel. Petratos v. Genentech Inc.,* 855 F.3d 481, 490-92 (3d Cir. 2017); *United States ex rel. McBride v. Halliburton Co.,* 848 F.3d 1027, 1033-34 (D.C. Cir. 2017); *United States ex rel. Kelly v. Serco, Inc.*, 846 F.3d 325, 334 (9th Cir. 2017). In *United States v. Sanford-Brown, Ltd.,* 840 F.3d 445, 447 (7th Cir. 2016), the Seventh Circuit panel concluded that where the Government had reviewed an allegedly fraudulent enterprise several times, but found no need to terminate

continued on page 15

continued from page 14

the contract or apply administrative penalties, the alleged fraud could not have been material to the decision to make payment.

In a recent case, *United States ex rel. Harman v. Trinity Indus. Inc.*, No. 15-41172, 2017 WL 4325279 (5th Cir. Sep. 29, 2017), the Fifth Circuit overturned a $663 million judgment against Trinity Industries, Inc. (Trinity), a guardrail manufacturer. The *Trinity* panel embraced *Escobar's* heightened materiality standard. The relator has filed a petition for a rehearing en banc, arguing the panel ignored Supreme Court precedent and ignored and reweighed evidence.

In *Trinity*, The Federal Highway Administration (FHWA) reimbursed states for installing guardrail end terminal systems that meet the FHWA's standards. During the time period at issue, eligibility for federal reimbursement required FHWA acceptance of the installed product. The FHWA could require product testing, and required any changes to approved systems to obtain "approval unless an exercise of good engineering judgment finds they were not significant." The FHWA approved Trinity's guardrail end terminal system, ET-plus in 2000. In 2005, Trinity made changes to the system and the FHWA approved the modified version. However, Trinity omitted some of these changes from a crash test report submitted to the FHWA for approval. When Trinity sold an ET-Plus system (often to state departments of transportation) it often submitted a certificate stating that the system complied with the FHWA testing requirements with its invoices. The complaint alleged that the undisclosed changes to the ET-Plus system violated the FHWA testing requirements, so Trinity's certifications that ET-Plus systems complied with those requirements caused states to present the FHWA with false claims for reimbursement.

Although no single factor was outcome determinative, the *Trinity* panel held that there was compelling and unrebutted evidence the FHWA knew about these issues but continued routine payments; consequently, the relators could not establish that the changes were material to the Government's decision to pay the claims. The appellate court distinguished this case from other post-*Escobar* appellate court opinions, emphasizing the seriousness and clarity of the Government's decision. First, the Fifth Circuit noted "*Escobar's* cautions have particular bite" when violations "involve potential for horrific loss of life and limb," such as the alleged violations regarding Trinity's guardrail system. Second, the *Trinity* court recognized that instead of inferring approval from continued payment as other circuit courts have post-*Escobar*, it could cite the Government's explicit approval. The FHWA issued a memorandum in 2014 expressing its continued approval of the ET-Plus system and identified "an unbroken chain of eligibility for Federal-aid reimbursement." At that time, the FHWA had actual knowledge of the alleged violations because its officials had seen the relator's thorough pre-filing presentation and had access to his *qui tam* complaint. The same day the FHWA released its memorandum, the Department of Justice responded to the relator's *Touhy* request, indicating no need for government employees' sworn testimony because the FHWA memorandum addressed all of the issues the parties raised. Accordingly, the Fifth Circuit held that the FHWA had actual knowledge of Trinity's alleged noncompliance with its 2005 changes, yet it continued to pay states' reimbursement claims for ET-Plus

continued on page 16

continued from page 15

systems. Thus, the relator failed to satisfy his materiality burden and Trinity was entitled to judgment as a matter of law.

Also noteworthy, the panel seemed to endorse the net trebling approach for calculating damages, although it did not identify the method by name. Under the pro-defense "net trebling" methodology, the value to the Government of the defendant's performance is first subtracted from the single damages figure before calculating treble damages. Contrastingly, the pro-government "gross trebling" methodology trebles the Government's alleged damages *first*, and then makes a reduction for any value received. Here, the appellate court explained the appropriate measure of calculation for damages is "the difference between what was promised and what was received."

Nonetheless, courts still critically apply the materiality standard based on the unique facts of each case:

- *United States ex rel. Escobar v. Universal Health Servs., Inc.*, 842 F.3d 103 (1st Cir. 2016): The First Circuit panel in *Escobar*, on remand, concluded that the relator met the materiality threshold. The relators alleged that a health care provider violated the FCA because it submitted Medicaid claims for reimbursement but failed to disclose employees lacked proper supervision or licenses and impliedly certified that its services complied with applicable requirements regarding employee qualifications. The Court held that the provider's misrepresentations were material because regulatory compliance was a condition of payment and the "very essence of the bargain," and there was no evidence that the Government had actual knowledge of the violations when it paid the reimbursement claims.
- *United States ex rel. Campie v. Gilead Sciences, Inc.,* 862 F.3d 890 (9th Cir. 2017): The Court reversed a Rule 12(b)(6) dismissal where the defendant contended that the Federal Drug Administration (FDA) continued to pay for HIV drugs despite knowledge that they did not meet manufacturing requirements. The case alleged: (1) Gilead manufactured drugs in an unapproved Chinese facility but charged the Government for them; (2) by selling these "knock-offs" to the Government and causing others to seek reimbursement for them, Gilead implicitly certified that the drugs were approved for distribution; and (3) Gilead lied to the FDA to secure approval of the Chinese manufacturing facilities, making them eligible for government payments. The court held the relators sufficiently plead materiality because: (1) it was unclear whether Gilead obtained the FDA approval by fraud; (2) there are many reasons the FDA may decide not to withdraw a drug approval; and (3) continued government approval here lacked the significance it has in other cases because Gilead ultimately replaced the noncompliant drugs with compliant drugs, the Government approved the compliant drugs, and the parties disputed the Government's actual knowledge.
- *United States v. Luce,* No. 16-4093, 2017 WL 4768864 (7th Cir. Oct. 23, 2017): The Seventh Circuit panel applied *Escobar's* "demanding" standard and held

continued on page 17

continued from page 16

> materiality was satisfied despite evidence of the Government's actual knowledge when approving payments. This case involved the owner and president of a company that was a Federal Housing Act (FHA) loan correspondent, who received FHA insurance for originating approved loans. The United States alleged the individual violated the FCA because he signed and submitted the company's annual certifications, lying about being subject to a current criminal proceeding. Although the Government had actual knowledge of the fraud and approved FHA insurance on new loans, the court explained this "acquiescence" was not prolonged because the Government subsequently initiated debarment proceedings resulting in debarment. The court cited additional evidence supporting materiality, including that (1) the certification at issue was a threshold eligibility requirement and thus linked to every loan issued; and (2) the failure to submit the Yearly Verification Form would have resulted in termination of FHA approval.

Important Takeaways for a Contractor's Strong Defense

This "demanding" materiality standard is important for contractors legally and practically. Importantly, the same facts that may defeat the materiality element may also defeat the scienter element. As the *Escobar* Court noted (in dicta) the scienter requirement for an FCA claim is "rigorous," too. The "government knowledge defense" can rebut the scienter element "under some circumstances . . . on the ground that the claimant did not act knowingly, because the claimant knew that the Government knew of the falsity of the statement and was willing to pay anyway." *United States ex rel. Colquitt v. Abbott Laboratories*, 858 F.3d 365, 379 (5th Cir. 2017) (internal quotation marks and citations omitted). This overlap in facts makes it imperative for defendants to approach discovery aggressively. It also further demonstrates the importance, during contract performance, of documenting with the Government any resolution of disagreements surrounding compliance or differences in interpretation of requirements.

Conclusion

More than a year after *Escobar*, litigants and courts continue to grapple with FCA materiality. Several appellate courts have embraced *Escobar's* heightened materiality standard, making it more challenging for FCA plaintiffs to satisfy their burden. Under this rigorous standard, the Government's actual knowledge and continued payment are key to defending against materiality because the Government's approval can be inferred from continued payment. Express approval, although present in the extreme *Trinity* case, is not required. This emphasizes the need for documentation during performance and aggressively pursuing discovery from the Government. ■

For more information, please contact:

Roderick L. Thomas
202.719.7035
rthomas@wileyrein.com

Michelle B. Bradshaw
202.719.7290
mbradshaw@wileyrein.com

Speeches & Publications

Current Enforcement Environment for Federal Grantees

April 3-5, 2018 | Arlington, VA

Annual Grants Training (AGT) 2018

John R. Prairie and Brian Walsh, Speakers

2018 Government Contracts Year in Review Conference

February 20-23, 2018 | Washington, DC

Rand L. Allen, Speaker

Applying New Department of Justice Compliance Standards to the Managed Care Context

February 12, 2018 | Scottsdale, AZ

2018 Managed Care Compliance Conference

Ralph J. Caccia, Speaker

Materiality and Implied False Certification: Split Circuit Decisions and the Impact of Escobar on Pending and Future False Claims Cases

January 29-30, 2017 | New York, NY

5th Advanced Forum on False Claims & Qui Tam Enforcement

Roderick L. Thomas, Panelist

Health Care Fraud Anti-Kickback Statue & Stark Compliance

December 7, 2017 | Atlanta, GA

Georgia Health Care Fraud Institute

Ralph J. Caccia, Speaker

Federal Grants Symposium

December 6-7, 2017 | Orlando, FL

Public Contracting Institute

John R. Prairie, Speaker

Government Contracts Statutes, Regulations, Executive Orders and Policies

December 2017 | Online Webinar

PubKLaw's Annual Review

Rand L. Allen, Speaker

Bid Protest Committee Meeting

November 21, 2017 | Washington, DC

ABA Section of Public Contract Law

Paul F. Khoury, Panelist

Final Rule on Paid Sick Leave for Federal Contractors and Subcontractors

November 13, 2017 | Online Webinar

Lorman Education Services

Eric W. Leonard, Craig Smith

E-Discovery in Government Contracts

November 8, 2017 | Washington, DC

ABA Section of Public Contract Law's Young Lawyers Committee and Contract Claims and Dispute Resolution Committee

Mark B. Sweet, Panelist

The Government Contract Intellectual Property Workshop

November 6-8, 2017 | Arlington, VA

Federal Publications Seminars

Scott A. Felder, Speaker

continued on page 19

Events & Speeches *continued from page 18*

ABA Section of Public Contract Law, Fall Meeting—From the Backstretch to the Finish Line and Contested Results—Bid Protests
November 3, 2017 | Louisville, KY
American Bar Association Public Contract Law Section
Kara M. Sacilotto, Moderator

Hot Topics & Emerging Trends in Litigation
November 2, 2017 | Washington, DC
Court of Federal Claims Advisory Council Panel Presentation
Paul F. Khoury, Panelist

Federal Acquisition Regulation Workshop
November 1, 2017
M.C. Dean's Fall 2017 Tech Expo
John R. Prairie, Speaker

Handling a Criminal Healthcare Fraud Case
October 29, 2017 | Washington, DC
HCCA's 3rd Annual Healthcare Enforcement Compliance Institute
Ralph J. Caccia, Speaker

Federal Grants: Navigating Compliance and Regulatory Requirements As Well As Cost Allowability Considerations
October 26, 2017 | Boston, MA
Federal Publications Seminars
Kendra P. Norwood, Speaker

Grants Update: OMB Super Circular 2 CFR Part 200
October 19, 2017 | Virtual Training
Public Contracting Institute
John R. Prairie, Speaker

Fun with the FAR (FAR Parts 3 and 9)
October 18, 2017
Public Contracting Institute
Kara M. Sacilotto, Speaker

About the Foreign Corrupt Practices Act and How to Enforce It
September 28, 2017 | Washington, DC
Trade-Based Financial Crimes Symposium
Kevin B. Muhlendorf, Panelist

Grants: Where Do I Start and How Do I Start Them
September 26, 2017 | Alvernia University, Reading, PA
Association of Fundraising Professionals
John R. Prairie and Brian Walsh, Speakers

Back to School – Protest Musings and Updates from Your Co-Chairs
September 19, 2017 | Washington, DC
ABA Public Contract Law Section, Bid Protest Committee Monthly Meeting
Brian Walsh, Panelist

continued on page 20

Events & Speeches *continued from page 19*

Introduction to Government Contracts Course
September 6-7, 2017 | Washington, DC
American Bar Association Section of Public Contract Law
Kara M. Sacilotto, Faculty Member

Six Modest Reforms for the Bid Protest Process
September 12, 2017 | ARTICLE
Bloomberg BNA's Federal Contracts Report
John R. Prairie, J. Ryan Frazee

Federal Sick Leave Health and Welfare Benefit Changes Bring Enhanced Compliance Challenges for Federal Service Contractors
September 2017 | ARTICLE
Wiley Rein and The Boon Group
Eric W. Leonard, Nina Rustgi

Going Retro: Back Pay Under the Service Contract Act
August 22, 2017 | ARTICLE
Bloomberg BNA's Federal Contracts Report
Eric W. Leonard, Craig Smith

Federal Grants: Navigating Compliance and Regulatory Requirements as well as Cost Allowability Considerations
August 16, 2017 | San Diego, CA
Federal Publications Seminars
George E. Petel, Speaker

Trends and Best Practices in Commercial Item Determinations
August 10, 2017 | New York, NY
American Bar Association Section of Public Contract Law Annual Meeting
Tracye Winfrey Howard, Moderator

DOD Announces Acquisition Reorganization Efforts *continued from page 13*

process in the near term. But here are two things industry can do to help make this effort succeed, as well as to stay current with processes that can affect companies' interests.

1. Pay attention to acquisition process infrastructural changes. Be on the lookout for modifications to key DOD acquisition-related documents—monitor changes as reflected in the formal rule-making process as well as in less formal changes to best practices by important agency stakeholders.
2. Where possible, participate in the change. How DOD will actually implement its goals and objectives remains unclear, so timely, thoughtful and balanced input from industry could actually result in changes that make a positive difference. At a minimum, pursuant to FAR 1.102(c) and FAR 15.201(c) contractors, as integral members of the acquisition team, are encouraged to take a role in achieving a better acquisition process. ■

For more information, please contact:

Richard B. O'Keeffe, Jr.
202.719.7396
rokeeffe@wileyrein.com

Lindy Bathurst
202.719.7287
lbathurst@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
Tracye Winfrey Howard	202.719.7452	twhoward@wileyrein.com
Matthew J. Gardner	202.719.4108	mgardner@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
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
Gregory M. Williams	202.719.7593	gwilliams@wileyrein.com
Jennifer S. Zucker	202.719.7277	jzucker@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	202.219.7394	mbroder@wileyrein.com
Katherine Campbell	202.719.7583	kcampbell@wileyrein.com
Colin Cloherty	202.719.3564	ccloherty@wileyrein.com
J. Ryan Frazee	202.719.3751	jfrazee@wileyrein.com
Sarah Hansen*	202.719.7294	shansen@wileyrein.com
Cara L. Lasley	202.719.7394	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 Rustgi	202.719.3761	nrustgi@wileyrein.com
Craig Smith	202.719.7297	csmith@wileyrein.com
Tara L. Ward	202.719.7495	tward@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