Wiley Rein LLP

GOVERNMENT CONTRACTS ISSUE UPDATE

February 2016

Government Contractor Cybersecurity Requirements and Guidance Continue to Evolve

Jon W. Burd and Cara L. Lasley

Over the last six months, cybersecurity guidance and requirements for government contractors continued to evolve, with significant developments for U.S. Department of Defense (DOD) contractors and the announcement of imminent new rules for civilian agency contractors. These developments will continue to have a profound impact on compliance efforts contractors are undertaking to secure government information that resides on contractor information systems. This article provides an overview and update on these developments, first for defense contractors and then for their civilian counterparts.

DOD Rules for Safeguarding Information Continue to Evolve

Following the November 2013 final rule implementing DOD's requirements for Safeguarding Unclassified Controlled Technical Information (UCTI), which adopted select standards from NIST Standard Publication (SP) 800-53 as the baseline for securing UCTI residing on contractor systems, DOD issued an interim rule on August 26, 2015, that made sweeping changes to the scope of the rule and the baseline requirements. *See* 80 Fed. Reg. 51739. Among the most significant changes:

DOD revised its baseline security standards from NIST SP 800-53 to a new NIST standard, SP 800-171, that was prepared specifically for government contractor systems and finalized earlier in the summer.

The interim rule expanded the scope of information that contractors will be obligated to secure using the revised security standards in NIST SP 800-171, to include not only UCTI but also "Covered Defense Information" including "critical information," "export control" information, and "[a]ny other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls."

DOD clarified that a contractor's safeguarding obligations extend not only to information received from the Government during contract performance, but also to any covered defense information that is "collected, developed, received, used, or stored by or on behalf of the contractor in support of the performance of the contract." Likewise, DOD clarified that the safeguarding obligations apply to covered defense information regardless of whether it was previously marked with a restricted distribution legend prior to receipt by the contractor.

continued on page 8

ALSO IN THIS ISSUE

Three Lessons for Federal Grant Recipients from Recent False Claims Act Investigations

By Mark B. Sweet and John R. Prairie

The U.S. Department of Justice and agency Offices of Inspector General continue to use the False Claims Act as a hammer against federal grant recipients that fall short of compliance with the terms and conditions of their awards. The good news is that every time the Government announces one of these settlements, it provides a lesson for other grant recipients in where the potential exposure lies. In this article, we take a look at several recent settlements and draw three lessons from them:

1. Good causes are not immune to liability.

It is natural to assume the Government will go easy on nonprofit organizations that use grants to further good causes, or that employees of charitable organizations will forgive each other for compliance miscues. But, as recent cases show, those assumptions are mistaken. A few weeks ago, a children's charitable organization was forced to pay $1.6 million to settle a False Claims Act investigation after an audit by the Inspector General revealed the organization had commingled grant funds with its general operating funds.

Last summer, a children's hospital had to pay $12.9 million to settle allegations that it misreported its available bed count on an application for a grant from the U.S. Department of Health and Human Services to fund pediatric residents training at the hospital. The misstatement was brought to the Government's attention by a hospital employee whose responsibilities included regulatory analysis and compliance. The employee received almost $2 million from the settlement.

2. The Government will follow the money trail especially when you don't.

One consistent target of law enforcement is grant recipients who fail to closely track funds received from the Government or misrepresent how they have spent those funds. Often these cases arise when the grant recipients have insufficient accounting and financial controls. For example, an Ivy League university paid $9 million to resolve concerns that it had not verified whether salary and wage charges were based on an employee's actual effort for that grant. To manage the multiple federal, state, and private grants funding the work it was doing, the university allegedly developed a system where its finance department created reports that allocated its employees' time across the many grants. The principal investigators on the grant then allegedly certified large batches of the reports as correct without inquiring with the employees who performed the work whether the time reports were accurate. The batch timekeeping system led to mischarging among federal, state, and private grants.

In November 2015, another university paid almost $20 million to settle allegations that it violated the False Claims Act. The Government alleged that the university did not have documentation to back up the level of effort claimed by hundreds of employees on the grants and that the university charged some of the grants for administrative costs for equipment and supplies that should not have been direct charges.

continued on page 3

continued from page 2

3. Don't cross funding streams.

Many research institutions receive grants from a number of sources at the same time. While multiple revenue streams can boost productivity, they can also create risks, especially when the different grants are similar in nature or the same employees work on multiple grants at the same time. As discussed above, one university struggled to track and allocate timekeeping among its multitude of federal, state, and private grants. A California university, meanwhile, had to pay $500,000 to resolve allegations that, in applying for a new grant from the U.S. Department of Energy, the university failed to disclose its overlapping research funded by a grant from the National Science Foundation. The university allegedly later submitted progress reports and renewal applications to the National Science Foundation listing accomplishments achieved under the Department of Energy grant.

Early this month, an astrophysicist paid $180,000 and entered into a deferred criminal prosecution for failing to disclose on a grant application that, in addition to working at his private company, he was full-time employed at a university. The scientist also understated how many other grants and competing time commitments he had with other federal agencies.

In each of these cases, the Government pursued damages and penalties under the False Claims Act because the grant recipient's representations and certifications did not accurately reflect its practices. Most likely, none of these targets ever considered itself to be "defrauding" the Government and came into the grant with the best of intentions. But unlike with traditional concepts of fraud, a grant recipient does not need to specifically intend to defraud the Government in order to be liable under the False Claims Act. Rather, in a False Claims Act case, the Government merely has to show that the grant recipient "knowingly" submitted a false claim or false document. That means an organization can violate the False Claims Act by recklessly disregarding or deliberately ignoring the truth or falsity of the information provided to the Government.

In the absence of sufficient internal controls, this can be surprisingly easy to do. To manage these risk areas and minimize exposure to False Claims Act liability, grant holders should consider conducting more employee training, hiring an internal compliance manager, performing regular audits, developing procedures to verify representations and certifications before they are made to the Government, establishing an employee code of conduct and disciplinary policies, and creating a hotline or website for employees to report fraud, waste, and abuse. ■

For more information, please contact:

Mark B. Sweet
202.719.4649
msweet@wileyrein.com

John R. Prairie
202.719.7167
jprairie@wileyrein.com

Déjà vu? Revised EEO-1 Report to Replace Proposed Equal Pay Report for Federal Contractors

Todd A. Bromberg and Jillian D. Laughna

On February 1, 2016, the U.S. Equal Employment Opportunity Commission (EEOC) published a proposed revision to the Employer Information Report (EEO-1) that would require employers, including federal contractors, with 100 or more employees to report pay information beginning in 2017. 81 Fed. Reg. 5113 (Feb. 1, 2016). For federal contractors, this proposed revision by EEOC may conjure a feeling of déjà vu. Back in 2014, the U.S. Department of Labor's (DOL) Office of Federal Contract Compliance Programs (OFCCP) similarly proposed requiring large contractors to submit compensation data in an annual Equal Pay Report. 79 Fed. Reg. 46562 (Aug. 8, 2014). Fortunately for contractors, the proposed EEO-1 revision moots the 2014 proposed rule because OFCCP plans to utilize EEO-1 pay data instead of requiring a separate Equal Pay Report. As with that now-moot 2014 proposal, the intent of the revised EEO-1 is to assist EEOC and OFCCP in identifying possible pay discrimination and assist employers in promoting equal pay in their workplaces.

W-2 Earnings Data and Pay Bands

Currently, the EEO-1 requires federal contractors with at least 50 employees and private employers with at least 100 employees to report annually the number of individuals they employ by job category, race, ethnicity, and sex for any pay period prior to September 30. Beginning in 2017, the proposed EEO-1 change would require large contractors and private employers with 100 or more employees to also submit data on employees' total W-2 earnings and hours worked. Through the use of W-2 earnings data, EEOC contends that employers will be able to provide pay data that they already maintain in existing human resource information systems (HRIS), without needing to collect any new data. Unlike the proposed Equal Pay Report, the revised EEO-1 proposes to aggregate pay data in 12 pay bands for the 10 existing EEO-1 job categories. For example, an employer would report on the EEO-1 that total hours worked for 10 African American men who are Craft Workers in the second pay band ($19,240-$24,439) is 10,000 hours. EEOC maintains that the use of pay bands will allow the agency and OFCCP to compute within-job-category variation, across-job-category variation, and overall variation, thus allowing the agencies to discern potential discrimination while preserving confidentiality.

Hours Worked and Burden Statement

The new requirement to collect information on hours worked will, in theory, allow EEOC and OFCCP to analyze pay differences by taking into account periods of time when employees were not fully employed, such as when an employee worked part time or for less than the full year. EEOC maintains that this will impose a minimal burden on employers because total hours worked data is maintained by almost all payroll systems. EEOC specifically seeks detailed employer input with respect to how to report hours for salaried employees. The agency notes that it is not proposing to require an employer to begin collecting additional data on actual hours worked for salaried workers, and proposes an approach where employers use an estimate of 40 hours per week for full-time salaried employees.

EEOC also seeks employer input on its calculation of the burden of complying with the proposed revision. The agency estimates that the total burden for filers submitting the revised EEO-1 amounts

continued on page 5

continued from page 4

to 6.6 hours for reading instructions and collecting, merging, validating, and reporting the data electronically for a cost of $159.92 per respondent (using the Bureau of Labor Statistics administrative support hourly rate of $24.23). In addition, there is an estimated one-time implementation burden cost for submitting the new pay and hours worked data amounting to $377.76 per respondent. This calculation is based on the one-time costs for developing queries related to the new data in an existing HRIS, which is estimated to take 8 hours per filer at a wage rate of $47.22. For public comment, EEOC encourages employers to provide: (1) quantitative information about the burden associated with completing the current EEO-1, as well as the anticipated burden to submit the new pay and hours worked data, and (2) data regarding the estimated time that staff will spend to report the new data and the corresponding wages for that staff. Comments on the proposed EEO-1 revisions are due by April 1, 2016.

Confidentiality

EEOC and OFCCP maintain that the agencies' will protect the pay data as required by law. EEOC holds EEO-1 data confidential as required by Section 709(e) of Title VII. It does not publish individual EEO-1 reports and publishes only aggregated EEO-1 data in a manner that does not reveal any particular employer's or employee's information. EEOC asserts that it will examine the rules for publishing aggregate data to ensure that tables with small cell counts – *i.e.,* the pay for one or two Hispanic or Latino women who are Executive/Senior Level Officials and Managers – are not made public. OFCCP will likewise protect the contractor data it receives to the maximum extent permitted under the Freedom of Information Act (FOIA).

Implications and Preparation

Like OFCCP's 2014 Equal Pay Report and 2011 data collection tool proposals, the proposed EEO-1 fails to address some key issues. The proposal specifically states that EEOC and OFCCP plan to use the pay data to assess complaints of discrimination, focus agency investigations, and identify existing pay data to assess complaints of discrimination. However, the collection and analysis of raw W-2 earnings data, which does not include information on factors such as education, experience, or performance that may affect pay, may lead to "false-positive" findings of pay disparities. These false-positives would likely lead to increased, and ultimately needless, OFCCP compliance reviews, requiring a significant effort by contractors to defend. In regard to confidentiality, although EEOC and OFCCP maintain that they will protect compensation data to the maximum extent possible, there is no guarantee that the data will be exempt from a FOIA request or data breach. Pay data in a competitor's hands could cause significant commercial harm.

In light of the Obama administration's emphasis on fair and equal pay, contractors should review their HRIS to prepare the systems to track and report the newly required data. The proposed EEO-1 Form to collect compensation data is available on EEOC's website at *http://www.eeoc.gov/employers/eeo1survey/2016_new_survey_2.cfm.* Contractors should also consider conducting a self-audit of their compensation data, practices, and manager training with outside counsel under the attorney-client privilege to identify and resolve any potential compensation discrimination exposure. ■

For more information, please contact:

Todd A. Bromberg
202.719.7357
tbromberg@wileyrein.com

Jillian D. Laughna
202.719.7527
jlaughna@wileyrein.com

When Submitting a Proposal, Late Is Late. Now, Even Early May Be Late If the Proposal Gets "Spammed."

By Philip J. Davis and Nina Rustgi

Offerors must overcome numerous hurdles in preparing and submitting proposals on a timely basis. A recent decision by the U.S. Government Accountability Office (GAO) has added yet another, and unexpected, obstacle – offerors now must be aware of and plan for the kidnapping of an otherwise timely proposal by an agency's spam filter.

It is a well-established principle that offers submitted after the submission deadline will not be considered for award, unless the circumstances specified in the FAR permitting acceptance of a late offer are met. The FAR is clear that the obligation is on the offeror to submit the proposal on time: "Offerors are responsible for submitting offers, and any modifications, revisions, or withdrawals, so as to reach the Government office designated in the solicitation by the time specified in the solicitation." FAR 52.212-1. Applying this principle in a recent decision, *Advanced Decisions Vectors, Inc.*, B-412307, Jan. 11, 2016, the GAO ruled that a contractor failed to timely submit its quote when the contractor's email containing the quote was blocked by the agency's spam filter from reaching the individual designated to receive quotes by the time specified in the solicitation. The decision serves as a warning to contractors that even an early submission of an offer may be ensnared by the tentacles of a spam filter and deemed late if it does not reach the intended recipient by the deadline as a result.

The *Advanced Decisions Vectors* decision stems from a U.S. Department of Homeland Security (DHS) procurement for analytical, statistical, consulting, and program management services that was issued through the U.S. General Services Administration's e-Buy system to vendors holding contracts under a particular Federal Supply Schedule. In the solicitation, the agency specified that quotations must be submitted electronically to a contract specialist (whose email address was provided) by no later than 10:00 a.m. on a particular day. On the due date, the contractor allegedly submitted its quote to the contract specialist's email address at 9:55 a.m. and also uploaded its quote to the e-Buy system. According to the agency, the contractor's email was caught by a series of email security services that sit between the DHS headquarters and the Internet and was never transmitted to the contract specialist. Rather, it was deleted by the DHS security system within a week per standard procedures. The contractor did not follow up with the agency until more than a month later, at which point it learned that its offer was never received and award had been made to another party.

The GAO rejected the contractor's arguments that its quote should be considered timely submitted because it was uploaded to the e-Buy system and because it emailed the contract specialist with its quote five minutes before the submission deadline. The agency was not notified of the contractor's submission to e-Buy and, furthermore, e-Buy was not the designated destination for the quote. As for the email caught by the spam filter, the GAO concluded that the record was clear that the contract specialist did not receive the contractor's quote by the submission deadline. In addition, because the email was deleted as a matter of course from the DHS system, the GAO was not able to verify that the email sent by the contractor to DHS actually contained the quote. Ultimately, the GAO denied the protest.

continued on page 7

Advanced Decisions Vectors provides several useful lessons for contractors when submitting an offer, including:

- If you have any questions or concerns about submitting an offer electronically, contact the agency well in advance of the deadline to resolve those questions or concerns. This can be done through the question and answer process or by contacting the point of contact designated in the solicitation directly.
- Submit your offer as early as possible. This will give the agency adequate time to confirm receipt and the contractor sufficient time to respond to any technical issues that may arise with the submission. (The GAO in *Advanced Decisions Vectors* noted that protester did not receive the confirmation promised in the solicitation.)
- If you do not receive written confirmation that the agency has received your offer before the submission deadline, contact the agency. In *Advanced Decisions Vectors*, the GAO did not look kindly on the fact that the contractor took no steps to ensure that its quotation was received by the agency until more than a month after submission.
- If after contacting the agency to confirm receipt you do not receive a timely answer, send the offer again. As the GAO emphasized, the responsibility is on the offeror to submit the offer in time.
- Confirm that you are submitting the offer to the proper recipient, location, or email address identified in the solicitation. If the offer is submitted to the wrong location, even if it was submitted by the deadline, this will not help you.

These steps can protect against an otherwise timely proposal getting caught in an agency's spam filter and, unbeknownst to the offeror, never reaching the addressee and being disqualified or not considered for award. ■

For more information, please contact:

Philip J. Davis
202.719.7044
pdavis@wileyrein.com

Nina Rustgi
202.719.3761
nrustgi@wileyrein.com

continued from page 1

Given the significant expansion in scope, industry expressed concern with both the immediacy of the interim rule and the lack of flexibility to implement the new NIST 800-171 requirements, many of which require corporate investment and planning to efficiently implement. Following a public meeting on December 14, 2015, DOD issued another interim rule on December 30, 2015, that provided flexibility in phasing-in the new baseline. *See* 80 Fed. Reg. 81472. The revision allowed for a two-year phase-in period for contractors to implement the adequate security requirements outlined NIST SP 800-171, and requiring contractors to implement those standards "as soon as practical, but not later than December 31, 2017." DOD was sensitive to the need "to provide immediate relief from the requirement to have NIST 800-171 security requirements implemented at the time of contract award," as contractors would otherwise be "at risk of not being able to comply with the terms of contracts that require the handling of covered defense information" upon contract award under the initial interim rule.

Notwithstanding the phase-in period, contractors must still notify DOD within 30 days after contract award "of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award," with an undertaking to implement the necessary standards later. This will enable DOD to monitor compliance trends and determine whether further revisions are warranted. Contractors will also have the flexibility to consider implementing "[a]lternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection," with written authorization by a representative of the DOD Chief Information Officer. This will provide additional flexibility for contractors that lack the organizational structure or resources needed to implement discrete requirements.

DOD's interim rules also create new obligations for contractors that plan to utilize cloud-based computing services to meet government information technology (IT) services requirements. Contractors that will fulfill DOD IT services requirements using a cloud-based solution must specify that plan in their proposals and obtain contracting officer approval. Among the requirements that DOD imposed, cloud-based service providers must:

- Obtain provisional authorization from the Defense Information Systems Agency (DISA);
- Provide access to the relevant data, contract personnel, and related facilities during any government audit, inspection, investigation, or similar activity;
- Store all government cloud-based data within the United States, unless the data is physically located on DOD premises or the contracting officer grants prior approval.

Cloud-based information services will be subject to cyber incident reporting requirements involving any cyber incidents, discovery of malicious software, spillage, or requests for access to data from third parties, including from any federal, state, or local agency. In the event of a cyber incident, contractors must preserve images of all known affected systems for at least 90 days after the submission of the cyber incident report, and provide DOD access to any information or equipment necessary for a forensic analysis.

OMB Proposed Guidance

In August 2015, the Office of Management and Budget (OMB) released proposed Guidance intended to improve cybersecurity for "controlled unclassified information" (CUI) that resides on contractor information systems. The Guidance came on the heels of the massive U.S. Office of Personnel

continued on page 9

continued from page 8

Management (OPM) data breach earlier in the year, and appears to piggy-back on many of the developments DOD implemented in its UCTI rule. The proposed Guidance was expected to be reissued in "the Fall" as "final" Guidance, but the final Guidance remains a work in progress. Ideally, any final Guidance, as well as any rulemaking by the FAR Council to implement the Guidance, will take into consideration the same challenges and need for flexibility that DOD adopted (albeit belatedly) with its December 2015 interim rule.

In general, OMB's Guidance aligns with DOD's baseline, and will require government contractors who collect or maintain information on behalf of a federal agency to implement similar security controls, conduct security assessments, and report cyber incidents. The proposed Guidance distinguishes between systems that are "operated on behalf" of the Government including systems performing "outsourced" services and functions, versus contractor internal information services used to provide a product or service to the Government. The distinction is significant, and the consequence having a contractor system characterized as one "operated on behalf" of the Government will be potentially higher levels of data protection, reporting obligations, continuous monitoring requirements, and government audit/investigation rights:

- **Data Protection:** Systems that are operated on behalf of the Government will be required to meet the security baselines in NIST SP 800-53, with each agency determining whether its risk profile falls as the low, moderate or high-risk baseline. Systems that contain CUI will be required to meet the "moderate baseline" security controls. Contractor systems that process CUI incidental to developing a product or service will have to meet the baseline established in NIST SP 800-171.
- **Reporting Obligations:** Contractors operating systems on behalf of the Government will be required to timely report ***all*** cyber incidents, while contractors operating their own systems have to report only incidents affecting CUI.
- **Continuous Monitoring:** Contractors operating systems on behalf of the Government will have to deploy continuous monitoring software developed by the U.S. Department of Homeland Security, use other monitoring software selected by the agency, or develop proprietary software that meets minimum requirements and is approved by the agency. Contractors operating their own systems, by contrast, will have to deploy continuous monitoring software in a manner consistent with the NIST 800-171 guidance, and will therefore have more flexibility in developing or installing monitoring software suited to their unique system requirements.
- **Security Assessments:** The Guidance calls for the Government to conduct security assessments of contractor systems, obtain third-party assessments, or rely on contractor self-assessments. The Guidance suggests that the Government may be able to obtain "access to the contractor's facilities, installations, operations, documentation, databases, IT systems, devices, and personnel used in performance of the contract" to conduct security "inspection, evaluation, investigation or audit and to preserve evidence of information security incidents." Presumably, systems operated "on behalf of" the Government would be subject to more rigorous audit and inspection rights. The Guidance also suggests that agencies develop contract clauses that would require contractors to certify the sanitization of government data at the conclusion of performance.

continued on page 10

SPEECHES & PUBLICATIONS

"Reaching Out without Getting Burned: Navigating the Intersection of HIPAA and the TCPA"
Dorthula H. Powell-Woodson, Rachel A. Alexander, and Kathleen E. Scott, Speakers
Maryland State Bar Association Health Law Section
December 14, 2015 | Cheverly, MD

"CLE Seminar: False Claims Act: Enforcing USF Beneficiary Rules and Policing Fraud"
Mark B. Sweet, Moderator
Federal Communications Bar Association
January 20, 2016 | Washington, DC

"OMB Cybersecurity Guidance & Recent Trends in Government Contracting"
John W. Burd, Matthew J. Gardner, Speakers
Managed Health Care Compliance Association National Conference
February 2, 2016 | Las Vegas, NV

"Statutes & Regulations"
Rand L. Allen, Speaker
West 2016 Year in Review Conference
February 17, 2016 | Washington, DC

"Federal Grants in 2016: Do you Still Comply?"
John R. Prairie, Brian Walsh, Speakers
Columbia Books & Information Services
February 24, 2016 | Webinar

continued on page 11

Government Contractor Cybersecurity Requirements and Guidance Continue to Evolve

continued from page 9

- **Due Diligence Database:** The Guidance requires the U.S. General Services Administration (GSA) to maintain a "business due diligence information shared service." The stated goal of the due diligence service would be to allow agencies to have access to "comprehensive information about current and prospective contractors and subcontractors" in order to assess the contractor's potential cybersecurity risk. Based on the Guidance, the database sounds like it would operate similarly to a past performance database, but the Guidance did not provide any details regarding due process that would allow contractors to review data inputs to the database or challenge incorrect information.

The language in the draft OMB Guidance is broad and primarily policy-oriented. Ultimately, the proverbial devil will be in the details of whatever rulemaking efforts come out of the final Guidance that OMB issues. In the meantime, contractors must continue to be attuned to the risk that civilian agencies may begin to make their own interim interpretations of the draft Guidance and implement a hodgepodge of new Section H contract requirements that require compliance with NIST SP 800-53 or 800-171 requirements, along with cyber incident reporting and/or certification requirements. We expect significant development in this arena to continue to play out over the next 18 months, and will continue to provide updates and analysis as they unfold. ■

For more information, please contact:

Jon W. Burd
202.719.7172
jburd@wileyrein.com

Cara L. Lasley
202.719.7394
clasley@wileyrein.com

Speeches & Publications *continued from page 10*

"Intellectual Property in Government Contracts Workshop"
Nicole J. Owren-Wiest, Scott A. Felder, Instructors
Federal Publications Seminars
March 9–11, 2016 | Washington, DC

"VA Small Business and Minority Set-Asides"
John R. Prairie, Panelist
Federal Circuit Bar Association Government Contracting Summit 2016
April 27, 2016 | Washington, DC

"Effective Trial Techniques"
Paul F. Khoury, Panelist
Court of Federal Claims Judicial Conference
May 3, 2016 | Washington, DC

Wiley Rein Wins *Law360's* Government Contracts 'Practice Group of the Year' Award for 'High-Profile Wins' in a 'Variety of Forums'

Wiley Rein's prominent Government Contracts Practice has been named a 2015 "Practice Group of the Year" by *Law360* in one of the publication's hallmark annual awards. Selected for the honor for two years running, Wiley Rein was noted for its "high-profile wins representing diverse clients in a variety of forums," a key factor that set it apart from other government contracts practices in 2015.

Law360 cited Wiley Rein's work in a "blockbuster win" at the U.S. Court of Federal Claims, in which the firm prevailed in defending Boeing Co. from a bid protest for a $4.76 billion NASA contract to provide commercial spacecrafts to send astronauts to the International Space Station. The article also noted the firm's successful appeal to the Federal Circuit in a bid protest involving the U.S. Department of Health and Human Services' Recovery Audit Contractor Program, where the firm's client CGI is an incumbent contractor. In this "widely watched" and precedent-setting case, a three-judge panel was effectively persuaded by Wiley Rein that the government's attempts to modify the payment terms for recovery audit contracts violated the Federal Acquisition Regulation's rules for the acquisition of commercial items. *Law360* also cited a successful protest on behalf of Citrix Systems Inc. that forced the U.S. Defense Information Agency to withdraw a request for proposals for up to $1.6 billion in software licensing that would have favored a rival company.

According to the publication, partner and two-time *Law360* "MVP" winner Scott M. McCaleb, along with partners Paul F. Khoury, Rand L. Allen and William A. Roberts III—all of whom were interviewed for the article—said they viewed the group's "well-rounded success as the biggest highlight of the year." All four partners emphasized that the *Law360* recognition is a reflection on the consistently excellent work and effort of the group's younger partners and associates, who have distinguished themselves in the bar as top-notch advocates.

Law360 received 730 submissions for the series—now in its sixth year—and selected 184 winners across 30 practice areas for honors. Wiley Rein was one of the eighty law firms to receive one or more "Practice Groups of the Year" awards this year. In addition to Government Contracts, the firm's received honors for its Insurance, International Trade, and Telecommunications practices.

To read the full article, please visit http://bit.ly/1QSVeOE.

Government Contracts Team

PARTNERS/OF COUNSEL

Rand L. Allen, Chair	202.719.7329	rallen@wileyrein.com
William A. Roberts, III, Co-Chair	202.719.4955	wroberts@wileyrein.com
Rachel A. Alexander	202.719.7371	ralexander@wileyrein.com
Todd A. Bromberg	202.717.7357	tbromberg@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
Paul F. Khoury	202.719.7346	pkhoury@wileyrein.com
Eric W. Leonard	202.719.7185	eleonard@wileyrein.com
Kevin J. Maynard	202.719.3143	kmaynard@wileyrein.com
Scott M. McCaleb	202.719.3193	smccaleb@wileyrein.com
Richard B. O'Keeffe, Jr.	202.719.7396	rokeeffe@wileyrein.com
Nicole J. Owren-Wiest	202.719.7430	nowrenwiest@wileyrein.com
Dorthula H. Powell-Woodson	202.719.7150	dpowell-woodson@wileyrein.com
John R. Prairie	202.719.7167	jprairie@wileyrein.com
Kara M. Sacilotto	202.719.7107	ksacilotto@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
Robert L. Walker	202.719.7585	rlwalker@wileyrein.com
Jennifer S. Zucker	202.719.7277	jzucker@wileyrein.com

ASSOCIATES

Moshe B. Broder*	202.219.7394	mbroder@wileyrein.com
J. Ryan Frazee	202.719.3751	jfrazee@wileyrein.com
Jillian D. Laughna	202.719.7527	jvolkmar@wileyrein.com
Cara L. Lasley*	202.719.7394	clasley@wileyrein.com
Samantha S. Lee	202.719.7551	sslee@wileyrein.com
Margaret E. Matavich	202.719.7356	mmatavich@wileyrein.com
Kendra P. Norwood	202.719.7069	knorwood@wileyrein.com
George E. Petel	202.719.3759	gpetel@wileyrein.com
P. Nicholas Peterson	202.719.7466	ppeterson@wileyrein.com
Nina Rustgi	202.719.3761	nrustgi@wileyrein.com
Craig Smith	202.719.7297	csmith@wileyrein.com
Brian Walsh	202.719.7469	bwalsh@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: http://www.wileyrein.com/newsroom-signup.html

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