Wiley Rein LLP

GOVERNMENT CONTRACTS ISSUE UPDATE

November 2016

Managing Risk with Insider Threat Programs

By Matthew J. Gardner and Jennifer S. Zucker

On May 18, 2016, the Department of Defense (DoD) published Change 2 to the National Industrial Security Program Operating Manual (NISPOM). NISPOM Change 2 requires that all cleared contractors establish and maintain an Insider Threat Program no later than November 30, 2016. With that deadline fast approaching, this analysis provides a brief overview of the key components of the new NISPOM requirements and highlights five considerations contractors should have in mind when standing up an Insider Threat Program.

Overview of Insider Threat Program Requirements

Under NISPOM Change 2, the Defense Security Service (DSS) requires cleared contractors—both possessing and non-possessing facilities—to create an Insider Threat Program designed to "gather relevant insider threat information across the contractor facility (e.g., human resources, security, information assurance, legal) commensurate with the organization's size and operations." Industrial Security Letter 2016-02, May 21, 2016, at 2 (ISL 2016-02). To implement

continued on page 3

ALSO IN THIS ISSUE

View from Our Clients: Ready for Fair Pay and Safe Workplaces but Concerns Still Linger, Even with Recent Injunction

By Craig Smith and John R. Prairie

The federal government had planned to start applying Executive Order 13673, Fair Pay and Safe Workplaces, last week. The EO and implementing FAR Rule and Department of Labor Guidance promised significant new compliance burdens, principally through requirements to report certain types of findings that contractors have violated specified labor laws. But just before the Fair Pay requirements were slated to begin phase-in, a federal district court in Texas enjoined almost the entire implementation nationwide, and on October 25 the Office of Federal Contract Compliance Programs directed federal agencies "to take all steps necessary" to comply with the court's order and not to implement the new requirements "until receiving further direction."

continued on page 6

DOJ Releases Guidance for Business Organizations Regarding Voluntary Self-Disclosures in Export Control and Sanctions Investigations

By John R. Shane, Lori Scheetz, and Carolyn R. Schroll

On October 2, 2016, the National Security Division of the Department of Justice (NSD) issued a guidance document (the Guidance) memorializing NSD's policy for corporate voluntary self-disclosures (VSD) of willful, criminal violations of U.S. export control and sanctions laws and regulations. What was once a streamlined process—disclosing potential violations to the relevant U.S. government agency and receiving an automatic 50 percent penalty reduction—now requires careful consideration, as the Guidance encourages companies to voluntarily self-disclose willful violations to NSD's Counterintelligence and Export Control Section (CES) in addition to disclosing to other responsible agencies if they want to obtain the mitigating benefit of such disclosure.

In this regard, instead of making the VSD only to the appropriate regulatory authority, and waiting for that authority to involve CES as needed, a company, under the Guidance, is now encouraged also to present the VSD directly to CES when the company becomes aware of potential willful violations. A company that discloses to the Directorate of Defense Trade Controls (DDTC), the Bureau of Industry Security (BIS), or the Office of Foreign Assets Control (OFAC), but does not disclose to CES, is at risk of not receiving credit for its VSD.

The Guidance establishes three requirements for a disclosure to be deemed voluntary. First, the disclosure must be made prior to the violation imminently coming to light by other means. Second, it must be timely made to CES and the appropriate regulatory agency after a violation is discovered. Third, the company must disclose all relevant facts, including facts about individuals involved in the violations.

The Guidance also outlines how companies can reduce penalties based on full cooperation and appropriate remediation. The Guidance recommends that prosecutors first determine whether the business met the threshold requirement in the September 9, 2015 Deputy Attorney General (DAG) Memo on Individual Accountability (the so-called "Yates Memo"), which mandates disclosure of all relevant facts relating to the individuals responsible for the misconduct. Then, the prosecutor should analyze the company's cooperation, taking into account the particular circumstances of the case. For example, a smaller company does not need to conduct as extensive an investigation as a larger company. Full cooperation includes, but is not limited to: disclosing all facts proactively; preserving and collecting information; providing details about internal investigations; and making witnesses and documents available. Businesses that do not meet all of the cooperation criteria can still receive partial cooperation credit, but only if they meet the DAG Memo on Individual Accountability's requirements.

Cooperation is also a prerequisite for receiving credit for remediation measures. Remediation requires implementation (or strengthening) of an effective compliance program and disciplining responsible employees. It also requires recognition and acceptance of responsibility for violations, and implementation of measures to ensure the company avoids repeat violations.

Additionally, the Guidance describes certain aggravating factors that could lead to higher

continued on page 8

the plan, contractors must, by November 30, 2106:

- Establish an Insider Threat Program;
- Appoint an Insider Threat Program Senior Official (ITPSO) who is cleared to the level of the facility and who will complete the ITPSO training by November 30, 2016;
- Implement the workforce training requirements related to insider threat; and
- Self-certify to DSS that the Program can fulfill the insider threat requirements.

Once implemented, contractors have continuing obligations to gather and report relevant and credible information that indicates potential or actual insider threats. In addition, contractors will be required to monitor classified network activity and to conduct self-inspections of their Insider Threat Programs. Section Y of DSS's Self-Inspection Handbook for NISP Contractors provides a series of questions to guide contractors through the various requirements of the Insider Threat Program.

Crafting an Insider Threat Program

Based on our recent experience working with cleared contractors to implement effective Insider Threat Programs, below are five key points and best practices that we believe are consistent with the NISPOM requirements and help mitigate risk in the event of an insider threat.

1. Tailoring the Program to the Contractor's Size and Complexity

DSS has expressly recognized that Insider Threat Programs under NISPOM Change 2 can be right-sized to match the sophistication of the cleared contractor. See ISL 2016-02 at 1 ("DSS will consider the size and complexity of the cleared facility in assessing its implementation of an insider threat program to comply with NISPOM Change 2."). Accordingly, contractors will need to consider whether existing company policies and procedures are in line with the NISPOM or if changes, updates, or additional items are required.

In that regard, DSS has not mandated a set of rigid best practices. Rather, cleared contractors must design and implement a pragmatic plan that is commensurate with their operations and resources. While contractors will benefit from the flexibility to tailor an Insider Threat Program to their organizations' needs and resources, they should make a realistic assessment of what resources they can and should commit to an Insider Threat Program. In the absence of a check-the-box set of requirements, over-promising and under-delivering are significant risks, and contractors must resist the temptation to implement plans that are little more than "paper policies" that lack actual implementation.

2. Documenting the Program

Under NISPOM Section 1-202, cleared contractors must create a written Insider Threat Program and self-certify to DSS that the plan has been implemented and is current. See id. DSS has provided a sample template for an Insider Threat Program. DSS's template is fairly rudimentary, suggesting that DSS does not anticipate that Insider Threat Programs will require much in the way of documentation, unless or until specific threats or incidents drive the need for additional or more rigorous controls.

Nevertheless, we recommend that contractors consider providing more robust documentation of their Insider Threat Program that goes beyond the "bare bones" model DSS has outlined. The real test of the sufficiency of any Insider Threat Program will likely be in the aftermath of an incident where an employee or other insider has compromised classified information and the Contractor must answer for those actions.

continued on page 4

continued from page 3

Contractors may be able to mitigate the risks and liabilities of future insider attacks by thoroughly documenting a robust Insider Threat Plan. That way, post-incident, the contractor can make a credible claim that the incident occurred despite the contractor's efforts. From that point of view, the more detailed the documentation is, the better—so long as the contractor actually has the resources and institutional backing to follow through and implement the plan. Especially in the event of an insider incident, a contractor's failure to implement a plan that it documented will likely compound problems and could introduce additional risks (such as suspension/debarment and False Claims Act liability).

3. Monitoring Classified Network Activity

Contractors must implement information system security controls, such as user-activity monitoring, on classified systems in order to detect activity indicative of an insider threat. See NISPOM Section 8-100(d); ISL 2016-02 at 5. We anticipate that for most contractors, the information security controls components of an Insider Threat Program will be relatively easy to implement, because most cleared contractors have already implemented the cybersecurity protections required by NISPOM Section 8-100(d). The DSS ODAA Process Manual provides specific guidance for the auditing and monitoring of contractor classified information systems under User Activity Monitoring/ Auditing (6.7.1).

As such, we anticipate that many contractors should be able to leverage existing cybersecurity protections to meet the information security requirements. This is especially true as DSS has stated that contractors can tailor their Insider Threat Programs to the sophistication and size of the contractor. For example, NISPOM Section 8-303(b) requires contractors to apply technical controls to ensure that contractors "limit [Information Systems] access to authorized users . . . [and that] access must be limited to the types of transactions and functions that authorized users are permitted to exercise." This is a basic cybersecurity requirement and is almost certainly being employed by most cleared contractors. See NIST Standard Publication 800-53, rev. 4. AC-6 (control establishing principle of least privilege to govern user access to information systems).

4. An Insider Threat Program Is Not Just an IT Solution

While information security controls may be relatively easy for contractors to implement, we anticipate that the more difficult part will be ensuring that the contractor has committed sufficient human resources to the Insider Threat Program. NISPOM Section 8-302 requires contractors to implement "Operational Controls," which it defines as methods "primarily implemented and executed by people (as opposed to systems) . . . ." For example, Section 8-302(a)(3) requires contractors to "review audit logs . . . as a component of its continuous monitoring to determine if there are any personnel failing to comply with security policies and procedures . . . ."

As a technical matter, capturing basic data on user activity such as login failures is easy. In fact, many IT systems will log this type of information by default. But, at some point, a real person will need to review those logs to identify potentially malicious or suspicious activity, like differentiating an employee who misspelled a new password twice in a row from one who is systematically trying to guess coworkers' passwords; or an employee who is working late on an authorized project versus one who is accessing a system after-hours to evade detection. To be sure, there are evolving tools to help consolidate and streamline this audit review function, but they do not replace the human element altogether. The Insider Threat Program should be built

continued on page 5

continued from page 4

and implemented through a post-incident lens. A contractor does not want to be in a position of trying to explain in hindsight why audit logs showed suspicious activity, but that activity went undetected because no one was reviewing the logs.

Operational Controls, i.e., experienced people who are able to analyze data and assess threats, are critical. Similarly, DSS has stated that a valid Insider Threat Program must also take the physical facilities into consideration. See Section 8-302(b)(2) ("Protect the physical plant and support structure of [Information Systems]."). Even allowing for DSS's recognition that an Insider Threat Program can be tailored to the contractor's size and complexity, a purely technical solution will not be regarded as a competent program.

5. Reporting Obligations

Under NISPOM Section 1-300, contractors must report information "that may indicate the employee poses an insider threat." See also ISL 2016-02 (Contractors must report "relevant and credible information" regarding cleared employees.). Although the reporting requirement has been extended to insider threat information, the basic reporting requirements are the same as NISPOM's long-standing requirements. For example: information regarding cleared employees, to include information indicative of a potential or actual insider threat and which falls into one of the 13 adjudicative guidelines, must be reported when that information constitutes adverse information under NISPOM Section 1-302a; incidents that constitute suspicious contacts must be reported under NISPOM Section 1-302b; incidents that constitute information concerning actual, probable or possible espionage, sabotage, terrorism or subversive activities must be reported to the Federal Bureau of Investigation under NISPOM Section 1-301. As before, we would caution contractors to err on the side of over-reporting. In addition to protecting national security, contractors will be best served to have a strong history of proper reporting should an incident occur. ■

For more information on developing and implementing insider threat detection and avoidance programs, please contact:

Matthew J. Gardner
202.719.4108
mgardner@wileyrein.com

Jennifer S. Zucker
202.719.7227
jzucker@wileyrein.com

View from Our Clients: Ready for Fair Pay and Safe Workplaces but Concerns Still Linger, Even with Recent Injunction *continued from page 1*

The Government will likely appeal the preliminary injunction and then defend the entire regime vigorously at the district court. So the Fair Pay requirements continue to loom as a potential major compliance obligation. Against this background, we spoke to clients about what they have done to prepare for Fair Pay and, in light of the preliminary injunction, what their plans are going forward.

Biggest Fears about the Fair Pay Requirements

Our clients' foremost concern is the one question that the hundreds of pages in the Federal Register could not answer: how would the system actually work? They expressed concern about practical compliance issues, ranging from the "absolute apparent unfettered discretion" of the Agency Labor Compliance Advisors (ALCAs) in their analyses of reported violations, to the difficulty that government personnel would face in mastering the Fair Pay requirements given their "sheer volume." These contractors fear being stuck in a vicious cycle of misapplied labor laws, misunderstood facts, and misused (but essentially unchallengeable) discretion.

Other concerns arose as well. Clients expressed concern that they would be hamstrung in contesting allegations or adverse preliminary findings, no matter how unmeritorious, because of the risk that reportable "labor law decisions" would lead directly to blacklisting by risk-averse contracting officers and higher-tier contractors. To that end, one client saw private litigants in particular as perhaps having "undue leverage" to extract settlements of dubious claims by explicitly invoking the benefits of avoiding a labor law decision that would be reportable under Fair Pay.

Clients with high proposal volumes noted that their own internal Fair Pay systems would be new and relatively untested once compliance requirements go into effect. They are not sure whether their systems for distributing notices to proposal teams about labor law decisions would work as intended and as needed, for example.

Preparations for Compliance

Reports of clients' preparations for Fair Pay were as varied as their industries and business models. But we found one perhaps unsurprising constant: clients that operate in a more decentralized organizational structure reported expending much more effort to locate, analyze and coordinate the records needed for Fair Pay compliance. (These companies regularly noted that they had never previously been required to consolidate these records.) These companies identified multiple functions and data sources with potentially relevant information needed for compliance, with some separated organizationally, geographically, or both. Attempting to obtain relevant records extended proposal preparation time in these circumstances, though this extra effort did provide a helpful gauge of the future burdens to be expected if and when the Fair Pay requirements finally "go live."

Challenges in Preparing

Clients reported challenges establishing a uniform baseline of information and documents across all covered labor laws. In many cases, different departments track and keep records on actual and potential violations. These departments have varying styles, processes, needs, and constituencies. Consequently, different departments within an organization often varied in what records they kept, how they kept them, and how willing they were to share them outside the department. Developing the common informational baseline, an effort usually headed by the law department, often took multiple requests and clarifications.

continued on page 7

View from Our Clients: Ready for Fair Pay and Safe Workplaces but Concerns Still Linger, Even with Recent Injunction *continued from page 6*

In contrast, other contractors—even of similar size and revenue—expended much less effort because the contractors already had consolidated labor and employment practices. But before any conclusions are drawn about the relative benefits or tradeoffs of a centralized labor/employment function within a company, note that none of our survey participants reported consolidating these practices in response to the Fair Pay EO and rulemaking; they had long been consolidated so as to best satisfy existing corporate business needs and practices.

Some clients with decentralized systems discovered a related but unexpected challenge: determining which corporate legal entity was involved in a particular matter. Such determinations matter because the Fair Pay Final Rule required disclosing only those labor law decisions rendered against the legal entity seeking or performing a covered federal contract or subcontract. These clients found that decisions and underlying documents might refer to "Contractor" but not specify which particular affiliate was involved, "Contractor Co.," "Contractor, Inc." or "Contractor, LLC." The distinctions were not always apparent to the responsible contractor functions, and resolving the underlying allegations had often not required confirming or documenting the legal entity involved. As a result, multi-entity clients in some cases had to work backwards through a documentary chain to determine which entity was involved and thus might have to report particular labor law decisions upon being subject to the Fair Pay requirements.

Subcontractor Management

While their own preparations varied, contractors have been near-uniform in deferring preparation for managing covered subcontracts and being a covered subcontractor. They welcomed the Final Rule's planned phase-in of the Fair Pay reporting requirements to cover subcontracts awarded under prime contracts solicited beginning on October 25, 2017. They planned to avail themselves of the extra time to revise and finalize their own internal processes while pursuing and performing contracts as prime contractors, then turn next year to outreach up and down the supply chain. Clients did not report taking these plans off their calendars, most likely because of the uncertainty about whether, for how long, and in what form the injunction will remain in effect.

The Injunction, and What's Next

Contractors we surveyed, not surprisingly, unanimously agreed with the preliminary injunction. They agree with the U.S. District Court for the Eastern District of Texas that the EO and implementation reflect executive overreach, irrational rulemaking, and disregard for the underlying statutory schemes. One client noted in particular that with the "consequences" already available for "poor legal compliance" (e.g., suspension and debarment) and public reporting of violations already in place, the Fair Pay regime undermined contractors' ability to "litigate, appeal, and/or resolve" through mutual agreement any allegations "to the fullest extent" allowed by the covered labor laws. The Fair Pay EO had, in other words, rewritten the laws' balancing of interests as passed by Congress and signed into law by the President.

As for what comes next, contractors expect to pause, but not dismantle, their Fair Pay compliance initiatives. As one example, contractors plan to leave in place newly centralized tracking of potential and actual decisions finding violations of covered labor laws. They also plan to address active and future allegations with an eye

continued on page 8

View from Our Clients: Ready for Fair Pay and Safe Workplaces but Concerns Still Linger, Even with Recent Injunction *continued from page 7*

towards the Fair Pay consequences and compliance efforts. Although these contractors are hopeful that the injunction will ultimately become permanent, or that a new administration will redirect focus to efforts that have at least a plausible chance of improving compliance with labor and employment laws, the contractors remain on standby to lead Fair Pay implementation in case that possibility ever comes to pass.

For more information, please contact:

Craig Smith
202.719.7297
csmith@wileyrein.com

John R. Prairie
202.719.7167
jprairie@wileyrein.com

DOJ Releases Guidance for Business Organizations Regarding Voluntary Self-Disclosures in Export Control and Sanctions Investigations *continued from page 2*

penalties in spite of disclosure, cooperation, and remediation. Exporting certain items, such as those used to create weapons of mass destruction or those controlled for nuclear nonproliferation reasons, is an aggravating factor. Exporting to terrorist organizations or to hostile foreign powers are aggravating factors, too. Companies will also receive less credit when there are repeat violations, if upper management was knowingly involved, or if the company received substantial profits from the violations.

Examples of reduced penalties companies could receive include a non-prosecution agreement, reduced fines, reduced time of supervision, or no required monitors. The Guidance recommends that prosecutors determine which reduced penalties to provide based on a balancing of credits and aggravating circumstances. The hypotheticals in the Guidance show NSD anticipates narrowly tailored penalties based on all of the circumstances surrounding a company's disclosure, cooperation, and remediation.

Overall, the Guidance strongly suggests that NSD plans to exercise a more active role and earlier involvement in willful, criminal violations of export control and sanctions laws and regulations. Given the high stakes and penalties involved, businesses seeking to take advantage of credits for disclosure and cooperation must take into consideration the Guidance and ensure that CES is fully involved as soon as a potential willful violation is discovered. Companies that fail to follow the Guidance will be less likely to receive reduced penalties, even if they disclose and cooperate with other agencies. It will, therefore, be important to reevaluate and change current compliance policies and procedures to incorporate the CES component in the company's decision-making and reporting process.

For more information, please contact:

John R. Shane
202.719.7222
jshane@wileyrein.com

Lori Scheetz
202.719.7419
lscheetz@wileyrein.com

Carolyn R. Schroll
202.719.4195
cschroll@wileyrein.com

The Five Types of Post-Award Debriefings Every Government Contractor Should Know How to Execute

By Kendra P. Norwood

After months of tirelessly pursuing a government contract that is crucial to your business plans, you finally receive the agency's notice of award and offer for a debriefing. Whether you were selected for award or not, there are important strategic decisions to be made regarding the post-award debriefing, which must be requested in writing within three days of receiving the award notice to preserve the benefits of a "required" debriefing.

Debriefings play a critical role in negotiated procurements. Contractors typically have little time to prepare for debriefings, and there may be competing business interests in the debriefing process, so it is important to understand the strategic reasons for pursuing a debriefing as well as the mechanics and logistics involved. Every government contractor should have a system in place for participating in debriefings that maximizes the likelihood that, whatever the underlying business objectives may be, the debriefing will be successful.

Federal regulations require contracting agencies to provide offerors with timely-requested debriefings in FAR Part 15 procurements, and specify that the debriefing must include meaningful information and offer an opportunity for the contractor to ask relevant questions about the procurement. This makes the debriefing a strategically important event for the business. Because a required debriefing may also be an important milestone for the timeliness of a potential protest, it is also legally significant.

What a contractor hopes to accomplish through the debriefing process will depend on a variety of factors, including whether the contractor was selected for award and what actions, if any, the contractor intends to take as a result of the agency's award decision.

Keeping in mind that a contractor might have multiple and overlapping goals, the keys to success in any debriefing scenario are to (1) realistically assess the situation, (2) determine your debriefing goals, (3) tailor a plan to achieve those goals, and (4) execute the plan with professionalism and discipline. There are five basic types of post-award debriefings that every government contractor should consider—and be able to execute—depending on the circumstances the contractor confronts:

1. The "Pre-Protest" Debriefing

The pre-protest debriefing is for disappointed offerors that have already decided to pursue a protest challenging the agency's award decision. This is often the primary motivation when the notice of award or other indicators point to likely prejudicial agency error with respect to a critical contracting opportunity, or when the business has identified other reasons to pursue a protest, such as the strategic significance of a program. The primary goal of this debriefing is to collect information to position the company for a protest. The debriefing is not about convincing the Government it is wrong. It is about discovery. FAR 15.506(d) requires the Government to provide the overall evaluated cost/price, technical ratings, and past performance ratings for both you and the awardee, and to identify all of the significant weaknesses or deficiencies in your proposal. If the Government ranked the proposals, you are entitled to know the overall ranking of the offerors. The agency is also required to provide you with a summary of its rationale for award and reasonable responses to relevant questions. It is in responses to questions and the dialogue with the Government about its findings that you may

continued on page 10

be able to uncover the "little extra" to fuel the merits of the likely protest. It is most effective to try to engage the Government in a back and forth, and get them "off script" as early in the debriefing as possible. The worst that can happen is that they refuse to do so, which in itself may provide some insight. Common areas to explore include the specific areas of concern that are fueling the desire to protest the agency's rationale for assessing specific weaknesses, why important aspects of a proposed technical approach did not warrant strengths, the basis for any most probable cost adjustments or price-related risk adjustments, and the key discriminators between your proposal and the awardee's.

While it is important to plan ahead for any debriefing, advance planning is particularly important for this type of debriefing since you are, in essence, building the record upon which your protest will be based. Assuming an in-person or telephonic debriefing, at a minimum you should make the following preparations: (1) assemble a team comprised of the appropriate personnel (the question of whether in-house or even outside counsel should attend often involves a strategic choice; while their presence may arguably stymie free conversation, there are often some benefits as well); (2) assign roles (including designated speakers and a dedicated note-taker); and (3) develop a list of mostly open-ended questions to ask the agency. (Note that those previously–prepared questions often become secondary in the debriefing once you learn new information. The team should be agile and prepared to follow up on details first learned at the debriefing, not simply wedded to the prepared questions.)

For in-person debriefings, you should also make arrangements to have a dedicated space at the debriefing site to caucus as a team, outside of the Government's presence. For a telephonic debriefing, if any of your team members are participating remotely, you should have access to an alternate dial-in number for caucus purposes that is separate and distinct from the phone line being used with the Government. You should also make plans to convene all relevant stakeholders immediately following the debriefing to review your notes, confirm the protest grounds you will assert, and make assignments for the key tasks that will be required to get the protest on file within the five days usually allotted.

2. The "Fact-Finding" Debriefing

The fact-finding debriefing is for unsuccessful offerors that are not sure whether they will protest the agency's award decision. The primary objective for this type of debriefing is determining whether the agency appropriately followed the source selection procedures outlined in the solicitation and the FAR. As with any debriefing, you should be well-versed on both the terms of the solicitation and the contents of your proposal. This familiarity will help you be nimble to identify any inconsistencies or ambiguities in the Government's evaluation process or any departures from the stated evaluation scheme. While the Government has the right to determine the debriefing format, if an offeror is given a choice, in-person or telephonic debriefings are best for fact-finding because they provide opportunities to observe and interact with the Government that are not typically possible with a written debriefing.

A fact-finding debriefing is the perfect opportunity to assess any perceived risk the agency may have regarding its evaluation process and ultimate award decision. During an in-person or telephonic debriefing, offerors should pay close attention to any comments from the Government that indicate the agency deviated from the solicitation's stated evaluation criteria, as well as the nuances of word choice, body language and the tone of the agency's responses to your questions. You should also be on the lookout for any

continued on page 11

signs of uncertainty or doubt the agency may display. This sort of behavior could reflect the agency's awareness that its evaluation process was potentially flawed, and therefore might suggest the need to follow-up on certain lines of inquiry. If an agency is not prepared to provide answers to reasonable questions "on the spot," ask if the agency will hold the debriefing open to allow additional time to engage in follow-up questions and answers (and always confirm any extension of the debriefing in writing to preserve the timeliness of any potential protest).

As in any post-award debriefing, offerors are entitled to reasonable responses to relevant questions during a fact-finding debriefing. If the agency fails to meet this requirement and significant doubts remain as to the propriety of the award, a protest may provide an avenue for counsel to obtain relevant information that was withheld during your debriefing (it is likely that any information revealed in a protest will be covered by a protective order that will restrict access to such information). While an inadequate debriefing is not an independent basis for protest, GAO has noted that an agency's failure to provide reasonable responses to relevant questions "may unnecessarily cause an unsuccessful offeror to file a bid protest in order to obtain such information." *Del-Jen Educ. & Training Grp./Fluor Fed. Sols. LLC*, B-406897.3, May 8, 2014, 2014 CPD ¶ 166 n.5.

3. The "Lessons Learned" Debriefing

The lessons learned debriefing is for unsuccessful offerors who are not planning to protest their non-selection for award. While it is wise to always keep an open mind on the possibility of protesting an award, the primary objective of this debriefing type is to obtain feedback from the agency on your proposal that can improve your competitive position in future procurements.

As discussed above, FAR 15.506(d) requires the Government to inform you of any significant weaknesses or deficiencies identified in your proposal. Sometimes contractors will simply come out and ask the Government something along the lines of, "*We want to learn for next time what we could have done better*?" Often, government personnel try to avoid a question phrased that way on the grounds that it is asking for speculation. Questions that will help you obtain the same type of information during a lessons learned debriefing, without the typical shut down response, include: "*What was the basis for assigning weaknesses or deficiencies to our proposal for each evaluation factor? Were there any solicitation requirements we failed to address? Were there any specific considerations that precluded us from being selected for award? Was anything missing from our proposal?"* Although FAR 15.506(e) precludes the Government from providing "point-by-point comparisons" of your proposal with those of other offerors, learning about the weaknesses and deficiencies of your own proposal can still be a tremendous benefit. Just as important as learning about areas where an agency viewed the proposal as weak, use the opportunity to learn about what you did well and what the evaluators liked. All of this information can help strengthen your approach in future competitions.

4. The "Marketing Pitch" Debriefing

The marketing pitch debriefing is one in which a disappointed offeror takes advantage of the opportunity to meet with the agency during an in-person debriefing to promote their company. All debriefings are essentially marketing opportunities. Each debriefing type presents a chance for the contractor to showcase the company's competence, organization and professionalism, thereby helping to burnish its reputation for future procurements. But there are times when marketing

continued on page 12

is the overriding goal of a debriefing—for example, when little is at stake in the present procurement, but more significant contracting opportunities lie ahead.

While an offeror may have failed to win the contract at issue, a marketing pitch debriefing may allow the company to make a positive impression on the agency, which may serve it well in future procurements. This is particularly true for companies looking to make inroads with a new agency, because they do not have an existing contracting history with the agency or are a new company that may lack name recognition.

To execute an effective marketing pitch debriefing, an offeror should be prepared to present its company in the best possible light within the context of a debriefing. This means putting aside the disappointment of not being selected for award and focusing on the valuable opportunity to showcase your company before a captive government audience. To prepare for a successful marketing pitch debriefing, you should develop thoughtful questions that will allow you to highlight your company's relevant experience and competencies while obtaining the information you seek on your proposal's evaluation. The following is an example of such a question: *"Our company has outstanding CPARS on the six different federal contracts we included in our Past Performance proposal, which involved the same or similar services solicited in this procurement. Could you please explain how that information was used in the source selection process?"* Another aspect of the marketing pitch debriefing is building rapport with the government participants. Often some of the most meaningful exchanges take place between individuals from the respective contractor and government teams either before, or particularly after, the formal debriefing.

5. The "Dress Rehearsal" Debriefing

The dress rehearsal debriefing is strictly for offerors that have been selected for award. As the awardee, you have a vested interest in ensuring the agency's award decision is not disturbed by the protests of disappointed offerors. One way to do this is to help the agency prepare for debriefings with unsuccessful offerors by having a "dress rehearsal" debriefing with you. As the awardee, it is perfectly acceptable to request that the agency provide your debriefing first, before debriefing any of the disappointed offerors. During a dress rehearsal debriefing, it may be a good idea for the awardee to pose questions to the Government that disappointed offerors are likely to ask about the source selection and evaluation process. This includes any unexpected or "wildcard" questions that the Government may not have considered. Successful offeror debriefings provide an opportunity to discuss with the agency how a disappointed offeror could misconstrue an agency's answers to questions to create a potential protest issue. The agency will benefit from the opportunity to conduct a debriefing with a live, "friendly" audience, and the contractor will benefit from an opportunity to learn about how its proposal was evaluated and cultivate its relationship with the government customer.

Conclusion

By giving thought to the company's ultimate business objectives, you can adopt a debriefing strategy that will best facilitate those goals. As discussed above, these strategies will be dictated in part by circumstance—whether you won or lost the competition—and in part by short- and long-term business goals. Regardless of the underlying circumstances, contractors should be prepared to take full advantage of the valuable opportunities that post-award debriefings provide. ■

For more information, please contact:

Kendra P. Norwood
202.719.7069
knorwood@wileyrein.com

Threat of False Claims Act Suits Undermines Attempts to Focus Universities on Mission Rather than Administrative Compliance

By Brian Walsh, Margaret M. Matavich, and George E. Petel

When it comes to doling out federal taxpayer funds for research grants, the Government has a strong interest in preventing waste, fraud, and abuse. In its zeal to protect the public fisc, however, the Government can tip the balance towards inefficient and unnecessary oversight at the expense of focusing resources on the actual research. Additionally, this balancing act often has multiple actors within the Government, with different agendas on either side of the equation.

This article analyzes recommendations by the U.S. Government Accountability Office (GAO) encouraging funding agencies to continue their efforts to reduce the administrative burdens and costs imposed on research universities that receive federal grant awards. It also highlights the upswing in False Claims Act (FCA) suits against universities involving federal research grants. Ultimately, these competing interests—more efficient administration versus more aggressive enforcement—send mixed signals to grant recipients that any administrative flexibility offered by the funding agencies could be offset by increased exposure to enforcement actions, potentially undermining the gains of various streamlining initiatives.

I. GAO Identifies Need to Ease the Burden on Grant Recipient Compliance

In June 2016, GAO issued a report highlighting opportunities to streamline administrative burdens imposed on federal research grant recipients. GAO-16-573, Federal Research Grants: Opportunities Remain for Agencies to Streamline Administrative Requirements (June 2016). On September 29, 2016, the GAO issued written testimony summarizing the report for a hearing of the House of Representatives Subcommittee on Research and Technology of the Committee on Science, Space, and Technology. In accordance with Executive Order No. 13563 and in response to decades-long complaints from the research grant community, the Office of Management and Budget (OMB) and research funding agencies have undertaken efforts to reduce the administrative workloads and costs faced by universities. These efforts include government-wide standardization, delaying some pre-award requirements until after preliminary funding decisions have been made, and permitting more flexibility for universities to assess and manage risks related to some requirements. GAO's findings show that these initiatives have had only limited results. GAO recommended increased efforts, particularly in these three areas, to further reduce burdens on universities and enable them to better allocate limited administrative oversight resources to those areas that pose the greatest risk of improper use of government funds.

GAO noted that there were at least nine distinct categories of administrative requirements, beyond proposal writing and submission, imposed on grant recipients during the competitively awarded federal research grant life cycle. Various stakeholder organizations have raised concerns about the burden of these requirements, with at least one such organization finding that principal investigators were spending, on average, 42 percent of their time on administrative tasks rather than performing active research. Another study identified financial management, the grant proposal process, progress reporting, and personnel management as the most frequently cited areas of high administrative workload.

continued on page 14

Efforts to reduce this burden, however, face the competing goal of ensuring that grant funds are properly spent. For example, the primary effort at standardizing grantee administrative requirements was the issuance of OMB's "super-circular," the *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards* (Uniform Guidance). This guidance consolidated a number of OMB's prior circulars in an attempt to provide consistency among grant recipients, reduce the administrative burden, and reduce waste, fraud, and abuse by strengthening federal oversight. The funding agencies have implemented the guidance through various agency-specific regulations, agency guidance, and in the terms and conditions of individual grant awards, creating a patchwork of compliance obligations from one agency to the next. Because of the competing goals of the Uniform Guidance, grant recipients continue to cite increasing compliance costs as the additional requirements outweigh the streamlining efforts, especially when those streamlining efforts are undercut by significant variations in implementation across different agencies. These increased costs fall mostly on the universities because of a compliance cost reimbursement cap included in the Uniform Guidance.

A. GAO Identifies Common Factors Driving Administrative Burden

During its review, GAO conducted interviews with officials at six research universities to identify common factors that add to their administrative workload and costs. Three common factors GAO discovered were variations among agency implementation of the Uniform Guidance; detailed pre-award requirements; and increased prescriptiveness of certain requirements. These burdens fell on both the universities' administrative staffs as well as on the researchers themselves.

Variations in the implementation of the Uniform Guidance substantially increased costs. Especially for larger universities that receive grants from different funding agencies, variations in the implementation of the Uniform Guidance often require multiple processes, requiring researchers and administrative staff to spend time learning each agency's unique requirements, processes, and systems. The universities reviewed by GAO all reported significant investment in electronic systems to attempt to comply with these variations, especially at the pre-award stage where any minor noncompliance can often result in a rejected grant application.

Detailed pre-award requirements were another area of significant concern to university officials, particularly when the likelihood of selecting a proposal for funding is relatively low. Researchers, including principal investigators, reported that responding to proposals and the submission process contributed the most to their administrative workload. The burden is especially high when the details of a research project requested by the funding agency are still unknown, resulting in inefficient estimating and updating processes.

Lastly, the increased prescriptiveness of certain requirements through the implementation of the Uniform Guidance has forced universities to implement new and updated systems. For example, new purchasing system requirements, including more detailed competition requirements for purchases above the micro-purchase threshold, forced the universities to update their electronic purchasing systems to handle to the increased number of transactions. Prescriptive subrecipient monitoring was also identified by the universities as a significant burden, particularly where the Uniform Guidance provides no risk threshold for when grant recipients are required to prescriptively monitor subrecipient compliance and the subrecipients's resolution of audit deficiencies. GAO reported

continued on page 15

OMB's opinion, that some of this burden is based on an erroneous interpretation of the requirements by the universities. GAO noted that audit findings by the Health and Human Services (HHS) and NSF Offices of Inspectors General were often based on differences in how auditors, agencies, and universities interpreted requirements. The universities expressed concern that they must conservatively interpret the requirements in the way that they expect aggressive Offices of Inspectors General would, or else risk findings that unallowable or questionable costs were charged to the grant. This conservative position leads universities to defensively conduct more thorough reviews and audits than are necessary under the guidance.

B. Recommendations to Reduce the Administrative Burden

GAO also identified steps funding agencies have taken to address the compliance burden, but many of these efforts focus on post-award administrative reporting burdens rather than the more significant pre-award burdens. The steps identified include:

- A pilot program designed to continue the coordination between agencies to standardize financial and other reporting by grant recipients.
- The Office of Science and Technology Policy Research Business Models (OSTP RBM) working group is expanding a centralized portal where researchers can assemble biographical information required for proposal submissions, and there have been some efforts to standardize terms and conditions. This portal, however, has not been adopted outside NIH and NSF.
- Some agencies have established different pre-award phases, allowing grant applicants to submit initial proposal documents sufficient to allow the agency to make an initial funding determination, sparing the applicants from preparing and submitting unnecessary documents when there is no chance of award. For example, requirements related to budgeting, full biographical sketches, data management plans, and researcher mentoring and developing plans have been postponed until later in the pre-award phase. Despite these efforts, even the agencies that have adopted this approach have not extended it to all grant solicitations, and regulatory changes would be needed to further extend this effort.
- The Uniform Guidance requires the use of OMB-approved government-wide standardized forms for the reporting of financial and performance information from grantees. The Uniform Guidance also provides grant recipients some flexibility in meeting certain requirements, including:
  - "Expanded authorities" under the Uniform Guidance allow funding agencies to waive certain prior approvals necessary before recipients can make changes to project budgets.
  - Changes related to documenting personnel expenses, including the streamlining of the payroll certification process, resulted in an 80 percent reduction in the number of forms principal investigators were required to review.
  - Allowing the use of fixed-amount grant awards reduces recipients' cost accounting burden.
  - A change in the accounting for administrative support staff provided greater flexibility to assign staff to specific projects, freeing researchers to engage in more active research rather than complying with the administrative requirements.

On the other hand, other administrative requirements, such as the imposition of the

continued on page 16

mico-purchase threshold and subrecipient oversight requirements, limit grant recipients' flexibility. These limits unnecessarily force grantees to shift resources to the oversight of low-risk areas such as micro-purchases, historically unproblematic subrecipients, and insignificant financial conflicts of interests. GAO recommended that agencies update their regulations to set more flexible risk tolerance levels and to better evaluate the effectiveness of their risk response actions.

The GAO report was especially critical of the Government for not addressing variations between agencies. GAO criticized OMB and RBM for not doing more to limit the funding agencies' variations. RBM's response stated that without allowing for such variation, the agencies would simply not adopt RBM's proposals for standardized terms and conditions and processes. GAO conceded that these problems were in part driven by differences in statutory mandates by Congress, but stressed that even within those restraints, the agencies have more opportunities to standardize than they are engaging in at present.

II. False Claims Act Suits Are on the Rise in Grant-Funded Research Arena.

At the same time the administrative burdens on universities and other grant recipients are changing, *qui tam* whistleblowers, Inspectors General, and the Department of Justice are increasing their efforts targeting these recipients for false claims actions based on fraud, waste, and abuse, as the following cases demonstrate.

U.S. *ex rel.* Feldman v. van Gorp, 697 F.3d 78 (2nd Cir. 2012): *False statements in doctoral fellowship program application*. This FCA suit was initiated by a former Cornell University fellow who filed a *qui tam* suit alleging that a Cornell professor of psychiatry and Cornell University Medical College made false statements in both an initial grant application and all renewal applications for grant funding. The government funding at issue was from the T32 grant program, which is run by the NIH. Compliance with T32 grant funding requires recipient pre- and post-doctoral programs to train fellows "with the primary objective of developing or extending their research skills and knowledge in preparation for a research career." The defendants sought T32 funding for a fellowship program which would study neuropsychology and HIV/AIDS. As part of the application, defendants identified core curriculum courses fellows would take, named specific faculty members serving as key personnel, and explained that fellows would work with persons with HIV. In each annual renewal application, defendants largely reiterated this information and did not report significant changes.

The nature of the relator's false statements in this FCA suit was that Cornell did not provide the curriculum, resources, faculty members, or training as described in the grant application, nor did Cornell identify changes to the program in its renewal applications to correct NIH's understanding of how the funding was being used.

After the relator prevailed, defendants appealed to the Second Circuit Court of Appeals arguing that damages had been improperly calculated and asking the Second Circuit to consider how to measure damages in a FCA case where a contract between the Government and defendants did not produce a tangible benefit to the Government. The Second Circuit reasoned that "the Government bargained for something qualitatively, but not quantifiably, different from what it received." Using this reasoning, the Second Circuit held that the appropriate measure of damages was the full amount the Government paid based on materially false statements by defendants—which ***amounted to the entire amount of the grant***. Because defendants had to submit yearly renewal applications—which contained false

continued on page 17

statements—the Court determined that these annual false statements materially influenced NIH's decisions to renew Cornell's T32 grant.

U.S. ex rel. Feldman demonstrates how protracted a FCA suit can become: the defendants applied for the grant funding at issue in 1997; the relator filed a *qui tam* suit in 2003 (two years after having left the program); the complaint was unsealed in 2007 when the Department of Justice declined to intervene; discovery was completed in 2009; and defendants eventually appealed to the Second Circuit, which issued a decision in 2012. It took 15 years to ultimately resolve this FCA suit involving grant funding for pre- and post-doctoral training at Cornell University Medical College.

United States *ex rel*. Melissa Theis v. Northwestern University, et al., N.D. Ill., No. 09 C 1943: *False statements in NIH claim submissions for grant expenditures.* The relator, the individual defendant, and the Government reached a settlement in this *qui tam* suit, in which the Department of Justice intervened.

Northwestern University received grant funding from NIH for which the defendant served as the Principal Investigator for at least five grant awards. The relator, a purchasing coordinator for Northwestern's medical school, alleged that the Principal Investigator authorized and directed the spending of grand funds on goods and services that did not meet the NIH and OMB guidelines for grant funds. The allegations involved improper submissions of claims to NIH for grant expenditures, including professional and consulting services, airfare, conference registration fees, food, hotel, travel, and other expenditures for the personal benefit of the defendant and his family and friends, incurred in connection with grants as to which the defendant was the Principal Investigator. In settling the FCA suit against him, the defendant agreed to pay $475,000.

United States *ex rel*. Rose v. Stephens Inst., N.D. Cal., No. 09-cv-5966: *False statements in certifying compliance with grant requirement.* In this suit the defendant, Academy of Art University, allegedly fraudulently obtained funds from the Department of Education, by falsely alleging compliance with Title IV of the Higher Education Act (HEA). The HEA requires fund recipients to enter a Program Participation Agreement (PPA), which requires the recipient to comply with certain regulations. The *qui tam* relators, four admissions representatives, alleged that Academy of Art University had been and was continuing to violate the PPA incentive compensation ban, which prohibits payment of any commission or bonus based directly or indirectly on an employee's success in securing enrollments or financial aid. The case against AAU is proceeding under an implied false certification theory, and ultimately the court will decide whether AAU paid compensation solely on the basis of enrollment success, and in doing so, made an impliedly false certification to the Department of Education. Notably, the relators prevailed against defendant's motion for summary judgment, with the court applying the recent Supreme Court FCA case *Universal Health Servs., Inc. v. United States ex rel. Escobar*. The case is pending in the Northern District of California.

United States v. Columbia University, S.D.N.Y., 13 Civ. 5028: *False statement in billing for grant overhead costs.* Columbia and the Department of Justice reached a $9.5 million settlement involving the FCA case against Columbia University. Columbia's FCA trouble arose out of its use of NIH grant money, specifically how Columbia billed for its facilities and administrative (F&A) indirect costs. NIH places restrictions on how much F&A costs a grant recipient could charge, one of which relates to whether research is conducted "on-campus" or "off-campus." Columbia improperly collected the

continued on page 18

full F&A rate—allowed only for "on-campus" research—for research conducted "off-campus."

United States ex rel. Thomas v. Duke University, et al., W.D. Va., No. 4:13-cv-00017: *False statements in scientific research potentially used to obtain funding.* A recently unsealed *qui tam* complaint against Duke University and a Duke University scientist centers on research misconduct as a basis for a false claim, which is a fairly new concept in the realm of FCA litigation. The *qui tam* suit was brought by a former Duke biologist who participated in a review of the scientist's data after the scientist separately pled guilty to embezzling money from Duke University. The review led to more than a dozen scientific papers being retracted. The relator alleges that during his participation in the review of the data, he learned that researchers and staff members knew the defendant "doctored" almost all of the experiments in which she participated. The relator claims that Duke is liable for a false claim because Duke received approximately 50 grants totaling $82.8 million from agencies, including NIH and the Environmental Protection Agency (EPA), which either directly arose from the research misconduct or where the misconduct influenced the award of the grant to Duke. The case is ongoing in the Western District of Virginia.

III. Trying to Streamline Compliance While FCA Threats Loom Large.

It is easy to see why universities may be wary of accepting the responsibilities associated with federal research funding, given the compliance requirements and the increase in FCA litigation relating to grant funds. The threat of a looming *qui tam* suit coupled with the growing, changing compliance environments is likely to cause universities to do far more policing and far less research. After all, a trebled damage award and potentially decade-long lawsuit presents a greater threat to a university's finances and public reputation than fewer published research papers. This is unfortunate, since it is clear that GAO recognizes that universities should not be saddled with unnecessary compliance costs—both dollar costs and the cost of taking researchers away from their work in the name of administrative paperwork—in exchange for receiving funding to conduct research.

The diverse range of fraud and abuse in the university research space that gave rise to the cases summarized in Section II illustrates how even streamlined administrative compliance will not eliminate universities' focus on monitoring and oversight of grant funds, perhaps to the detriment of progress on research. While agencies have been working to streamline administrative compliance, all the myriad ways a false claim can be generated in the university research space are likely to keep universities feeling the burden of complying with federal funding requirements. However, this should not discourage or dissuade GAO and funding agencies from continuing to attempt to achieve meaningful progress in lessening the administrative compliance burden placed on universities. Indeed, perhaps lessening the administrative burden on universities will allow universities to shift that effort to monitoring true fraud and abuse while still allowing universities to accomplish their research initiatives. ■

For more information, please contact:

Brian Walsh
202.719.7469
bwalsh@wileyrein.com

Margaret M. Matavich
202.719.3756
mmatavich@wileyrein.com

George E. Petel
202.719.3759
gpetel@wileyrein.com

When an Employee Takes Proprietary Materials

By Todd A. Bromberg, Mark B. Sweet, and Dylan Hix

The risk that a current or departing employee will misappropriate proprietary company information is ever-present for government contractors. A government contractor employee might take company documents or data for any number of reasons. For instance, the employee could be planning to use the materials to gain a competitive advantage at the next job, or to sue the company for employment-related claims. An employee who believes the documents show fraud or other illegalities might hope to bring justice to a perceived wrong (or, perhaps more selfishly, for a big payday or publicity as a whistleblower).

To protect the company's proprietary information and legal rights, every government contractor should have a specific response plan for when it believes an employee has improperly taken company documents. This article provides concrete steps and important considerations for reacting to theft of proprietary materials, including a new federal law that empowers employers to take immediate action in federal court when proprietary information is stolen.

Investigate immediately

The first step when an employee may have taken documents is to conduct an immediate investigation directed by counsel. The company should lock down the employee's computer, devices, and accounts in order to prevent further misappropriation of documents and preserve the electronic record. The company should then begin a forensic investigation to assess the scope of the employee's misappropriation: what documents were taken, how were they accessed, what was done with them, and how can any gaps in data security protocols be closed to prevent further data exfiltration? If the activity involves a current employee, it may be necessary to place the employee on administrative leave pending the outcome of the investigation and any decisions on continued employment.

The company should also interview people who worked with the employee in order to understand potential motive and the risk of potential wrongdoing—for instance, whether the employee may be acting as a whistleblower based on previous expression of concerns of discrimination, fraud, or other potentially illegal conduct. The entire investigation should be directed by counsel to preserve confidentiality and privilege, ensure thoroughness, and lend credibility to the investigation in the event it becomes relevant in a subsequent government disclosure, investigation, or lawsuit.

Assess the legal implications and options

Once the company has a sense of what materials were taken, it should assess the legal significance of the materials and the company's legal options and obligations. Theft of trade secrets may provide grounds and good reason for immediate legal action. Under the Defend Trade Secrets Act (DTSA), which became federal law in May, a victim of trade secrets theft can file suit in federal district court and seek a number of remedies, including injunctive relief to prevent actual or threatened misappropriation, *ex parte* seizure of property to prevent the disclosure or dissemination of trade secrets, and money damages (including double damages and attorney's fees in some circumstances). Most states provide similar remedies under state law. If the theft occurred electronically, the Computer Fraud and Abuse Act may be a basis for a civil suit. The company may also have grounds to sue the individual for tort claims.

continued on page 20

continued from page 19

The company should also analyze any employment or non-disclosure agreements signed by the employee. These agreements may include liquidated damages or a right to seek attorney's fees if the company prevails in litigation. Short of litigation, the company can send a letter notifying a former employee of the grounds for liability and demanding immediate return of the materials. If it appears the former employee plans to use the company's proprietary information in employment with a competitor, the company should consider notifying the competitor as well.

If the company wants to be aggressive without necessarily taking on the full burden of civil litigation, it can refer the matter to law enforcement for a potential criminal prosecution. Indeed, notifying law enforcement may be required by federal and state regulations in some situations, such as when classified information, personal information, or health information has been misappropriated. If the stolen information belongs to or reveals confidences of a customer, notifying customers may be necessary as well.

The company may have other options if it learns about the misappropriation while the person is still employed with the company. The company's code of conduct and other policies likely spell out that misuse or disclosure of confidential company information is grounds for discipline, even termination.

While aggressive action is often justified and necessary to protect the company, the company may want to proceed more cautiously if the Government is involved or could become involved. Under the terms of its contract or the Federal Acquisition Regulation, the Government may own the intellectual property that has been stolen, which may limit the company's ability to claim a trade secret. Additionally, federal and state laws provide whistleblower protections that will require careful consideration. For example, the DTSA immunizes individuals from liability for confidentially disclosing trade secrets to government officials or to attorneys for the purpose of reporting or investigating suspected legal violations. Other statutes, such as the False Claims Act and Sarbanes-Oxley, prohibit retaliatory adverse employment actions against current employees who are engaging in protected activity. To the extent there might be a government investigation related to the company documents, aggressive action against the employee (whether current or former) could be viewed by the Government as an attempt to muzzle a whistleblower. In fact, if the company believes that the employee plans to share the information with the Government, the best response may be a proactive disclosure to the inspector general, contracting officer, or suspension and debarment official that provides appropriate context and puts the company in the best light possible.

In short, the company should assess all of its legal options while keeping in mind the potential consequences of going after a purported whistleblower—especially when viewed through the eyes of a government investigator. If aggressive action is still warranted, make sure to document the reasons and justifications for each step and consider briefing potential stakeholders before the theft or the company's response becomes public knowledge.

Strengthen compliance, training, and data security

Finally, an employee's misappropriation of company materials should be treated as an opportunity to learn about vulnerabilities and to prevent recurrences. Potential

continued on page 21

continued from page 20

whistleblowers often take company materials as a way of taking matters into their own hands because they voiced concerns but believe they were not heard. If this is the case—and regardless of whether the employee's concerns have merit—the company should consider strengthening its internal reporting channels and re-training employees on how to use them. The company should review its policies to make sure the definition of proprietary materials is clear and the policy is communicated routinely. Employees should be reminded of the potentially severe legal consequences of misappropriating trade secrets and other proprietary information. Finally, the company should assess whether the breach exposed vulnerabilities in data security that should be addressed. ■

For more information, please contact:

Todd A. Bromberg
202.719.7357
tbromberg@wileyrein.com

Mark B. Sweet
202.719.4649
msweet@wileyrein.com

Dylan Hix
202.719.7557
dhix@wileyrein.com

SPEECHES & PUBLICATIONS

New FOIA Improvement Act Increases Necessity for Contractors to Create Robust FOIA Exemption Record
Jon W. Burd, Tracye Winfrey Howard, George E. Petel
Pratt's Government Contracting Law Report
September 2016

Presentation on OMB Memorandum regarding Federal Source Code Policy
Moshe B. Broder
ABA Public Contract Law Section, Intellectual Property Committee
September 2016

Fraud Symposium on Fraud Investigations
John R. Prairie
InsideNGO
September 2016

DCode42 Presentation on Government Contracts Pricing
John R. Prairie, Nicole J. Owren-Wiest
DCode42
September 2016

SBA Mentor Protégé Programs Final Rule
George E. Petel, Speaker
ABA Section of Public Contract Law, Subcontracting, Teaming and Strategic Alliances Committee Meeting
September 7, 2016

Assessing Responsibility of Individuals: Industry Perspective
Paul F. Khoury, Moderator; Kara M. Sacilotto, Panelist
ABA Public Contracts Section, Suspension & Debarment Committee Meeting
September 16, 2016 | Washington, DC

You're on the Hook: Mitigating Compliance Risks in an Era of Proactive Subcontractor Management
Eric W. Leonard, Craig Smith, Speakers
Lawline
October 19, 2016

FUN with the DFARS Season 2
Nicole J. Owren-Wiest, Speaker
Public Contracting Institute
October 19, 2016

Federal Circuit Government Contracts Decisions Year in Review
Tara L. Ward, Moderator
Fedreal Circuit Bar Association, Bench & Bar Webcast
October 24, 2016 | Washington, DC

Spurring Innovation Through Non-Traditional Procurement Vehicles
John R. Prairie, Brian Walsh, Speakers
Association of Procurement Technical Assistance Centers Fall 2016 Training Conference
November 8, 2016 | Washington, DC

The Government Contract Intellectual Property Workshop
Nicole J. Owren-Wiest, Scott A. Felder, Speakers
Federal Publications Seminars
November 14-16, 2016 | San Diego, CA

Doing Business With DOD & The Intel Community - Behind Closed Doors
Jennifer S. Zucker
Jennifer Schaus & Associates
November 28, 2016 | Arlington, VA

Changes in Small Business Contracting
John R. Prairie, George E. Petel, Speakers
Fairfax County Bar Association, Government Contracts Section
December 1, 2016

Trends and Developments: Defending Commerciality and Price Reasonableness
Nicole J. Owren-Wiest, Tracye Winfrey Howard, Speakers
Association of Corporate Counsel National Capital Region, Government Contractors Forum
December 13, 2016

Claims, Disputes and Terminations in Government Contracting
Paul F. Khoury, Moderator
PubK Law Year in Review
December 15, 2016 | Washington, DC

Second Annual PubKLaw Year-In-Review FY 16/17
Rand L. Allen, Speaker
PubK Law Year in Review
December 15, 2016

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
Matthew J. Gardner	202.719.4108	mgardner@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
P. Nicholas Peterson	202.719.7466	ppeterson@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
Lori Scheetz	202.719.7419	lscheetz@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
Jennifer S. Zucker	202.719.7277	jzucker@wileyrein.com

ASSOCIATES

Moshe B. Broder	202.219.7394	mbroder@wileyrein.com
Colin Cloherty*	202.719.3564	ccloherty@wileyrein.com
John Fletcher*	202.719.3568	jfletcher@wileyrein.com
J. Ryan Frazee	202.719.3751	jfrazee@wileyrein.com
Dylan Hix	202.719.7557	dhix@wileyrein.com
Jillian D. Laughna	202.719.7527	jlaughna@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
Carolyn R. Schroll	202.719.4195	cschroll@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

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