Hogan Lovells

ADG Insights

Top 5 areas of False Claims Act risk for Aerospace, Defense, and Government Services companies

November 2019

Michael Mason, Jonathan Diesenhaus, Peter Spivack,
Stacy Hadeka, Michael Scheimer, and Rebecca Umhofer

The False Claims Act (FCA) today bears little resemblance to the law President Lincoln signed 154 years ago to stop con artists like those who sold the U.S. Army gun powder barrels filled with saw dust or boots with cardboard soles.

Today, companies and individuals in all sectors of the economy who do business with the government, or participate even remotely in government programs, face a growing common threat: the risk that a whistleblower will label them a modern day huckster for failing to comply with some regulation, triggering a costly and lengthy government investigation, and potentially a lawsuit for treble damages and substantial financial penalties.

FCA risk in the Aerospace, Defense, and Government Services (ADG) industry is particularly significant for several reasons. ADG companies frequently enter into contracts with U.S. government customers, and those contracts often require upfront disclosures of information as well as affirmative certifications or representations of compliance with federal regulations and quality requirements. Noncompliance with these disclosure and certification/representation requirements can trigger staggering liability under the FCA, staggering because under the FCA the government recovers treble damages and civil penalties between $11,463 and $22,927 per false claim. DOJ reports that $2.8 billion was recovered in FCA actions during fiscal year 2018, $2.1 billion of which was linked to suits filed by a whistleblower who stood to recover up to 30% of the government's recovery. FCA rewards in the ADG industry are often headline grabbing when they relate to the high cost systems and services that may also have national security implications.

This publication of ADG Insights addresses the five compliance topics that currently pose the highest risk of FCA liability for ADG companies. An understanding of this risk will help inform ADG companies on how to prioritize the elements of their compliance programs. The five risks addressed herein are:

1. Cybersecurity
2. Defective Pricing
3. Supply Chain Risk Management
4. Overbilling
5. Defective Quality of Products or Services

ADG companies will want to ensure that coverage of these areas in their compliance programs is especially strong.

Top risk areas for ADG companies

Cybersecurity

ADG companies are frequent targets of cyber attacks given their propensity to store sensitive technical data as well as other government information that has national security implications or that otherwise is of high economic value. In recognition of this fact, the federal government has imposed a framework of cybersecurity requirements that typically requires ADG companies to make substantial investments in infrastructure that meets certain data safeguarding standards. Given these requirements and the attention cybersecurity currently is receiving, noncompliance has become a prime target for FCA whistleblowers.

As discussed in our ADG Insights of April 2019, Cybersecurity and Supply-Chain Developments and Trends for Companies that Conduct Business with the U.S. Government, the government is applying increased scrutiny on contractor compliance with cybersecurity requirements, including how those requirements are flowed down to subcontractors. ADG companies that conduct business with civilian government agencies are subject to the requirements of the Basic Safeguarding of Covered Contractor Information Systems rule. The rule is implemented in Federal Acquisition Regulation (FAR) clause FAR 52.204-21, which identifies 15 security controls, pulled verbatim from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, for safeguarding information systems owned or operated by contractors that process, store, or transmit specified federal contract information (FCI). FCI is broadly defined as information "not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government," but excludes information provided by the government to the public or simple transactional information. The rule is intended to impose baseline cyber protections that the government believes every business should be implementing as a "best practice."

ADG companies that conduct business with the Department of Defense (DoD) are subject to more stringent cybersecurity and incident reporting requirements. DoD's Network Penetration Reporting and Contracting for Cloud Services rule applies to all DoD contractors and subcontractors, including small business and commercial item contractors, except contracts for the acquisition of commercial-off-the-shelf items. Covered contractors are required to safeguard Covered Defense Information (CDI) and "rapidly report" cyber incidents on contractor systems with CDI. CDI is defined broadly to include unclassified controlled technical information or other information as described in the Controlled Unclassified Information Registry. Contractors are required to provide "adequate security" on all covered contractor information systems, which means at a minimum, implementing the security requirements in NIST SP 800-171 by no later than 31 December 2017. Rapidly reporting is defined as reporting within 72 hours of the contractor's discovery of a cyber incident using the reporting fields at https://dibnet.dod.mil.

These rules pose significant risk of FCA liability where a contractor misrepresents its compliance status with the applicable cybersecurity requirements and does so knowingly or with reckless disregard. Two recent cases underscore this FCA risk for ADG companies.

- In July of this year, an OEM of video surveillance equipment (VSE) agreed to pay $8.6 million ($2.6 million to the federal government and $6 million to state government purchasers) to resolve FCA allegations that the company failed to meet cybersecurity requirements. The relator and government alleged that flaws in the VSE could allow hackers to take over the surveillance system and gain access to the entire networks of government agencies that had purchased the system. These security flaws allegedly rendered claims for payments for the VSE false under the federal and state false claims acts because: (1) the VSE's security flaws were so significant that they rendered the VSE worthless; and (2) the VSE's flaws violated numerous federal information processing standards.[1]
- In another FCA case, a leading ADG company faced allegations by a whistleblower (the company's former senior director of Cyber Security, Compliance, and Controls) that the company made false statements to the government relating to the level of its compliance with DoD and NASA cybersecurity requirements. After the Government declined to intervene in and adopt the

1. Joseph Marks, Cisco to Pay $8.6 Million Fine for Selling Government Hackable Surveillance Technology, Wash. Post (July 31, 2019) available here.

whistleblower's allegations, the company moved to dismiss, arguing that because it had disclosed its noncompliance to the government, the whistleblower (a/k/a relator) could not adequately allege that the noncompliance was material under the FCA. The court acknowledged that "if the Government pays a particular claim in full despite its actual knowledge that certain requirements were violated, that is very strong evidence that those requirements are not material."[2] The court, however, found that the relator adequately alleged that the company had not disclosed the full extent of its noncompliance. Moreover, the court held that even if the government never expected full technical compliance, the relator had properly pled that the extent of a company's compliance still mattered to the government's decision to grant it a contract and therefore the materiality pleading requirement was satisfied.[3]

Accordingly, in addition to posing a risk of loss of sensitive technical or other information, noncompliance with the ever-evolving cybersecurity requirements poses significant FCA and "headline" risks.

It is important for ADG companies to monitor the evolving nature of government-imposed cybersecurity requirements. As mentioned in our September 2019 ADG Insights, NIST Set To Enhance Contractor Cybersecurity Duties, NIST recently published SP 800-171B, which will supplement the baseline requirements contained in SP 800-171 by enhancing cybersecurity requirements for those contractors that handle high value assets or participate in critical programs on a contract-by-contract basis. DoD contractors should pay special attention to how these requirements will correlate with the DoD's new Cybersecurity Maturity Model Certification (CMMC) program. That program, which is expected to be implemented in 2020,[4] currently would subject contractors to third-party verification that they maintain the appropriate level of cybersecurity practices and processes and would make cybersecurity status a "go/no go" issue for bidding purposes. Although having a third-party independently verify the level of compliance should reduce the risk of FCA liability, there will remain risk to the extent that the contractor provides inaccurate information to the third party verifier or makes direct misrepresentations upon which the government relies.

Defective pricing

FCA allegations also arise when a contractor knowingly fails to provide current, accurate, and complete cost and pricing data in the course of negotiating a government contract. The two highest risk areas for the fraudulent or "defective" pricing type of FCA claims are (1) noncompliance with the requirement to submit current, accurate, and complete certified cost and pricing data under the Truth in Negotiations Act (TINA) and (2) failure to submit current, accurate, and complete commercial sales practices information under the General Services Administration's (GSA's) Federal Supply Schedules (FSS) program.

Noncompliance with the Truth in Negotiations Act

The TINA requires contractors and subcontractors to disclose current, accurate, and complete certified cost or pricing data when negotiating government contracts and subcontracts (and modifications thereto) in excess of $2 million, unless an exception applies. TINA defines the term "cost or pricing data" to mean all facts that, as of the date of agreement on the price of a contract (or the price of a contract modification), a prudent buyer or seller would reasonably expect to affect price negotiations significantly. This includes vendor quotations, nonrecurring costs, information on changes in production methods and in production or purchasing volume, data supporting projections of business prospects and objectives and related operations costs, unit-cost trends such as those associated with labor efficiency, make-or-buy decisions, estimated resources to attain business goals, and information on management decisions that could have a significant bearing on costs. The term excludes judgmental information, but includes the underlying verifiable facts. The statute provides a price reduction remedy

2. United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc., 381 F.Supp. 1240, 1246 (E.D. Ca. 2019) (quoting Universal Health Servs. Inc. v. United States ex rel. Escobar, 135 S.Ct. 1989 (2016)).
3. Id. at 1249.
4. Version 0.6 of CMMC was released on November 7, 2019. There is also an open DFARS case 2019-D041 for the Strategic Assessment of Contractor Protection of Controlled Unclassified Information, which will implement a standard DoD-wide methodology for assessing DoD contractor compliance with all security requirements in NIST SP 800-171.

for noncompliance that impacts the negotiated price, but TINA violations may also form the basis of an FCA claim.

This FCA risk is illustrated by a settlement agreement reached by a major defense contractor through which the contractor agreed to pay $3 million; and return "unallowable costs" to resolve allegations that it inflated parts and labor costs during contract negotiations with the U.S. Army. Specifically, the contractor allegedly provided government negotiators inflated costs for parts the contractor would need to purchase to fulfill the contract and inflated labor costs the contractor would incur if it built the parts itself. The government alleged that the contractor's knowing failure to disclose accurate cost and pricing data resulted in the Army agreeing to a higher contract price – a price it would not have agreed to had the contractor disclosed current, accurate, and complete cost or pricing data.[5]

In another case, an ADG contractor agreed to pay $13 million to settle claims that it falsely inflated the cost of military contracts to produce the Bradley Fighting Vehicle, an armored vehicle used in the Gulf War, and the M113 tank. The claim alleged, among other things, that the company falsely inflated the amount it intended to spend on independent research and development and bid and proposal projects. The complaint further alleged that the Army relied on those false statements and therefore reimbursed the contractor for greater expenses than it would have if it had known the contractor's actual spending plans.[6]

FCA case law reflects that not every expectation or hope of lower costs must be disclosed under TINA. This issue was litigated in U.S. ex rel. Sanders v. Allison Engine Co. There, a relator alleged the defendant, a first tier subcontractor, caused false claims to be submitted to the government by withholding cost and pricing data from the prime contractor. The Sixth Circuit Court of Appeals held that the defendant did not have to "relay its expectation or hope that it would have lower costs" during the contract negotiations. U.S. ex rel. Sanders v. Allison Engine Co., 471 F.3d 610, 626 (6th Cir. 2006), vacated and remanded on other grounds, 553

5. Bryan Koenig, Gov't, BAE Resolve Army Truck FCA Suit For $3M, Law360, (June 2, 2017), available here.
6. Press Release, U.S. Dep't of Justice, FMC Corp. Agrees to Pay $13 Million to Settle False Claims Act Allegations (Oct. 8, 1996), available here.

U.S. 662, 128 S. Ct. 2123, 170 L. Ed. 2d 1030 (2008). In doing so, the Sixth Circuit distinguished a case in which a defense contractor failed to disclose "sealed bids" from a potential supplier that it had in its possession but had not unsealed. Id. (distinguishing Aerojet Solid Propulsion Co. v. White, 291 F.3d 1328 (Fed.Cir.2002)).

The extent of FCA risk posed by TINA violations is expected to increase materially. In this regard, the Defense Contract Audit Agency recently announced that it intends to triple the number of TINA audits it conducts in FY 2020 (from 20 completed in FY 2019 to 60).[7] DCAA's increased focus on defective pricing underscores the importance that ADG companies focus on TINA compliance and the associated FCA risk as defense spending surges. ADG companies that are subject to TINA will want to ensure that they have strong processes in place to collect and disclose, including through the TINA "sweep" process, current, accurate, and complete certified cost and pricing data.

Noncompliance with the commercial sales practices disclosure requirements

ADG companies that sell commercial products and services on are frequently subject to unique pricing disclosure requirements that often form the basis of an FCA claim. Federal Supply Schedule (FSS) contracts, negotiated and managed by the GSA, are of strategic importance for many companies selling commercial products and services. With certain exceptions, companies negotiating an FSS contract must disclose their "commercial sales practices." Some of the largest FCA settlements involving government contractors involve allegations that the contractor failed to make a current, accurate, or complete disclosure of its commercial sales practices.

Examples of FCA settlements that highlight this risk include:

- A May 2019 settlement with a GSA contract holder in which the contractor agreed to pay $21.57 million to resolve allegations that it caused false claims by providing misleading information about its commercial sales practices during contract negotiations with GSA.
- A $45 million settlement with another GSA contract holder to resolve allegations that the company made false statements and claims about the discounts it gave to commercial customers.
- A $75.5 million settlement to resolve allegations that contractors violated the FCA by misrepresenting commercial pricing practices in connection with the sale of products and services offered under a reseller's schedule contract.
- An agreement to pay $199.5 million plus interest to resolve allegations that a contractor failed to meet its contractual obligations to provide GSA with current, accurate, and complete information about its commercial sales practices, including discounts offered to other customers.

Therefore, even those "commercially friendly" contracts can include pricing disclosure requirements that pose significant risk of FCA liability. It has become common practice for auditors and whistleblowers to allege after-the-fact that a contractor's disclosure of historical pricing information and practices is incomplete. Contractors will want to ensure that adequate processes are in place to produce sufficient disclosures, including capturing and describing the contractor's deviations from its standard commercial sales practices.

Supply chain risk management

ADG companies' have historically been required to comply with certification and representation requirements dictated by the Buy American Act (BAA), the Trade Agreements Act (TAA), and rules applicable to specialty metals, counterfeit electronic parts, and other areas that can impact sourcing decisions. Violations of these requirements have led to FCA investigations and significant liability. For example:

- On August 8, 2019, DOJ announced that a government supplier would pay $3.3 million to settle FCA allegations that it violated the TAA by selling products to the Defense Logistics Agency and the Department of Veterans Affairs that were made in China and Malaysia, which are not designated countries (i.e., not compliant) under the TAA. According to the DOJ press release, the company's executives certified that its products came from TAA compliant countries despite

7. Anthony Capaccio, Pentagon Plans to Triple Audits Amid Surge in Defense Spending, Bloomberg (Sept. 13, 2019) available here.

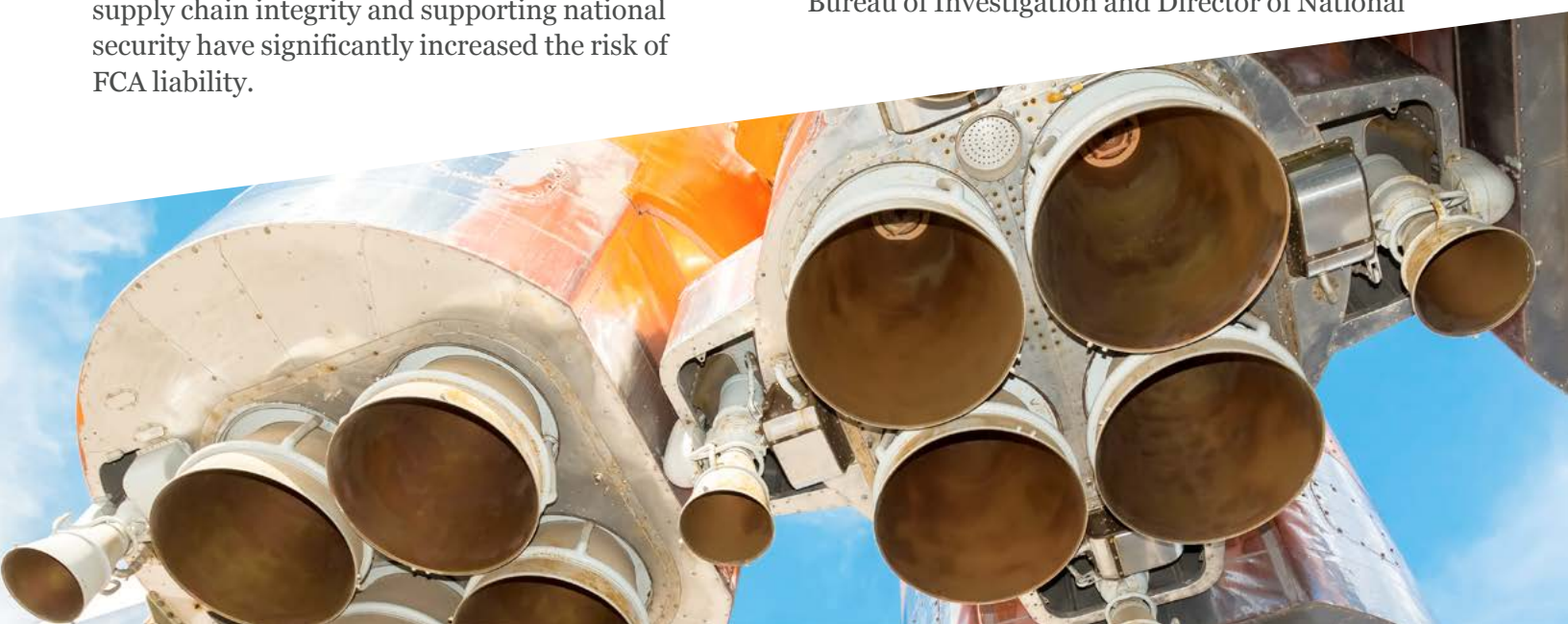
allegedly knowing that most of the products were manufactured in noncompliant locations.

- A major conglomerate agreed to pay $2.3 million to resolve allegations that it caused the submission of false claims for products sold on GSA contracts in violation of the TAA. Specifically, the settlement resolved allegations that, over an eight-year period, the company caused resellers of its products to sell items on their GSA contracts in violation of the TAA by knowingly providing inaccurate information to the resellers regarding the goods' country of origin.
- A reseller of technology software and hardware agreed to pay $5.66 million to resolve allegations that it submitted false claims in connection with a GSA contract. Specifically, the settlement resolved allegations that, between 1999 and 2011, the company improperly sold products that were manufactured in China and other non-TAA compliant countries.
- Finally an alleged violation of the specialty metal rules led to an aerospace company entering a $6 million settlement. That settlement resolved a suit brought under the FCA, which alleged the company delivered parts made of Russian titanium for use in military aircraft.

The list of supply chain-related compliance obligations for ADG companies doing business with the government continues to expand. As discussed above, the government also requires contractors to flow-down cybersecurity requirements to its subcontractors. Additionally, several recent statutory and regulatory requirements aimed at ensuring supply chain integrity and supporting national security have significantly increased the risk of FCA liability.

For example, sales of software and other products or services of Kapersky Lab to the government are prohibited. This prohibition includes use of Kapersky Lab software or hardware as a component of any solution sold to the government. Section 1634 of the National Defense Authorization Act (NDAA) FY 2018 (Pub. L. 115-91) prohibits agencies from directly or indirectly using any hardware, software, or services developed or provided in whole, or in part, by Kaspersky Lab. This statutory Kaspersky Lab ban was implemented via FAR clause 52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities. The clause is mandatory in all solicitations and contracts, and flows down to all subcontracts (including subcontracts for the acquisition of commercial items).

ADG companies are also prohibited from selling solutions containing certain telecommunications equipment, surveillance equipment, and related services to the government. Section 1656 of the FY 2018 NDAA prohibits the DoD from procuring or obtaining any telecommunications equipment, system, or service that relies on "covered items" to carry out the nuclear deterrence or homeland defense missions. Covered telecommunications equipment or services is defined as: (1) telecommunications equipment produced by Huawei Technologies Company or ZTE Corp. (or any subsidiary or affiliate of such entities); (2) telecommunications services provided by such entities or using such equipment; or (3) telecommunications equipment or services produced or provided by any other entity that the Secretary of Defense (in consultation with the Federal Bureau of Investigation and Director of National



Intelligence) reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a "covered foreign country" (defined in this section as China or Russia).

Section 889 of the FY 2019 NDAA, titled Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment, considerably expands on the prohibition contained in section 1656 of the FY 2018 NDAA. First, it expands the definition of covered items in Section 1656 of the FY2018 NDAA by not limiting the prohibited uses to nuclear deterrence or homeland defense missions. Instead, the prohibition now extends to all federal agencies (not just DoD), surveillance services and equipment, telecommunications equipment and services, and loans and grants as well as procurements of covered equipment. In one respect, however, the prohibition in Section 889 is narrower – a "covered" foreign country is defined in Section 889 as being China and only China (Russia is not included). Section 889 of the FY 2019 NDAA also prohibits (effective August 13, 2020) federal agencies from entering into a contract or extending a contract with an entity that uses any covered equipment or services as a substantial or essential component of any system. Section 889 is implemented, effective August 13, 2019, in FAR 4.2105 and FAR clause 52.204-24, which require contractors to certify that they will not provide prohibited products.[8] DoD, GSA, and NASA are currently working on 2nd interim rule to allow offerors to represent annually whether they sell equipment, systems, or services that include covered telecommunications equipment or services, and a proposed rule to further implement Section 889, which is anticipated by January 2020.

The clear trend in the government's approach to supply chain risk management reflects a continued expansion of government restrictions on the sale of technologies from certain entities that the government deems to present a national security risk. In addition to potentially garnering adverse publicity and having a negative impact on contracts, noncompliance with the current and future restrictions pose significant risk of FCA liability.

Overbilling

A case in which a government contractor overcharges the government has been recognized as "an archetypal qui tam False Claims action." See U.S. ex rel. Hendow v. Univ. of Phoenix, 461 F.3d 1166, 1170 (9th Cir. 2006). The FCA was indeed passed during the Civil War in response to such overcharges and other abuses by defense contractors. It is therefore no surprise that FCA claims alleging that a government contractor has overcharged the government are not uncommon and that allegations of overbilling take numerous forms, including billing for labor that does not satisfy the applicable labor qualification (e.g., education, experience) requirements, billing for more hours than worked, failing to pass through rebates or discounts to the government, and overstating costs incurred in performing the contract. Some recent examples include:

- In a 2019 settlement, a government service provider agreed to pay $5.2 million to resolve allegations that it billed the government for the work of personnel performing IT services at higher hourly rates than the personnel who performed the work were qualified for under the contract.
- In 2018, a major defense contractor agreed to pay $27.45 million to settle allegations that it violated the FCA by overstating the number of hours its employees worked on two contracts with the United States Air Force. Additionally, the company agreed to forfeit $4.2 million to resolve a criminal investigation into fraudulent billing on one of the contracts.
- In May 2017, a government service provider agreed to pay $95 million to resolve civil fraud claims and agreed to forgo administrative claims against the United States, which sought $249 million in additional payments. The government alleged that the company knowingly overcharged DoD for locally available fresh fruits and vegetables supplied to U.S. soldiers in Kuwait and Iraq by failing to disclose and pass through discounts and rebates it obtained from suppliers, as required by its contracts.

8. GSA has developed a class deviation to the applicability of FAR 4.2105, which limits the representation requirements to the Indefinite Delivery, Indefinite Quantity contract level instead of at the order-level for low and medium risk indefinite delivery contract vehicles. Per the deviation, GSA requires representation and reporting clauses in all new solicitations. The deviation also establishes implementation targets for modification of existing contracts to include both the representation and reporting clauses.

- One of the largest ADG global companies agreed to pay $23 million to resolve allegations that it submitted false claims for labor charges on maintenance contracts with the U.S. Air Force. The government alleged that the company knowingly and improperly billed a variety of labor costs in violation of applicable contract requirements, including for time its mechanics spent at meetings not directly related to the contracts.
- Another major defense contractor settled FCA allegations relating to labor mischarging. In that settlement, the contractor agreed to pay $9.2 million to resolve allegations that it knowingly overbilled the government for labor on U.S. Navy and Coast Guard ships. The settlement also resolved claims that the contractor had billed the Navy and Coast Guard for dive operations to support ship hull construction that did not actually occur as claimed.
- A company that manufactures antennae and radio systems agreed to pay $10 million to resolve allegations that it overcharged the U.S. Army for electronic warfare antennas. The company allegedly misrepresented its costs to manufacture the antennas, and thereby inflated the price the Army paid.

ADG companies must also be aware that the government has brought FCA claims against prime contractors even where the overbilling was caused directly by a subcontractor. For example, a leading ADG company settled an FCA claim that alleged the government was overcharged as a result of a seven-year pricing scheme by a subcontractor that sold perishable tools to the company for use on military aircraft. Specifically, the government alleged that the subcontractor inflated the costs of these tools and that the prime contractor purportedly acted recklessly by failing to adequately oversee the subcontractor's charging practices and by mishandling information revealing these practices.

There are many aspects relating to proper billing that should be addressed by a compliance system. Indeed there are many nuances that may need to be addressed, including mapping labor rates to the appropriate labor category; ensuring that billed labor

meet the qualification requirements for the applicable labor category; accurately capturing hours worked on a project; appropriate charging of fee and indirect costs; allocating to the government discounts, rebates, and refunds where appropriate; compliance with most favor customer pricing provisions, and many other government-imposed requirements.

Defective quality of products or services

ADG companies that conduct business with the government typically must meet stringent quality and testing standards that often are government-unique. These standards vary based on the product or service provided and may require not only that the product meet certain specifications, but also that the contractors certify that they have met specific testing and inspection requirements. Failure to deliver on these contractual promises can lead to FCA claims such as those described below.

- An Oregon aluminum extrusion manufacturer and its corporate parent agreed to pay $34.6 million in April 2019 to resolve FCA claims that the company caused a government contractor to invoice DoD's Missile Defense Agency and NASA for aluminum extrusions that did not comply with contract specifications. According to DOJ, the contractor admitted to providing customers, including U.S. government contractors, with falsified certifications after altering the results of tensile tests designed to ensure the consistency and reliability of aluminum extruded at the companies' facilities. The government investigation also resulted in a guilty criminal plea to one count of mail fraud and a deferred prosecution agreement in connection with mail fraud. To protect the government supply chain, NASA also suspended the contractor from government contracting and proposed the company for debarment government-wide. The company's exclusion from government contracting has been effective since Sept. 30, 2015.
- An FCA claim brought in the District of Connecticut, No. 3:13-CV-1730 (August 2018) by a former employee of a major engine manufacturer alleges the defense contractor used a defective spray coating process in the manufacture of jet engines for the Air Force. The complaint further alleges that the company manipulated contractually required test procedures and results.
- A government contractor agreed to pay $4.6 million to resolve allegations that it violated the FCA by knowingly failing to perform required quality assurance procedures and falsely certifying that those requirements had been met. The suit further alleged that one-third of the rebar supplied by the company and used in the construction of a Department of Energy (DOE) nuclear waste treatment facility was found to be defective.
- In November 2016, DOJ settled FCA allegations with three government contractors that allegedly made false statements and claims to the DOE by charging DOE for deficient materials, services, and testing that was provided to a nuclear water treatment plant. The companies allegedly improperly billed the government for materials and services from vendors that did not meet quality control requirements. The companies agreed to pay $125 million to resolve these allegations along with allegations that one of the companies improperly claimed and received government funding for lobbying activities in violation of the Byrd Amendment and applicable contractual and regulatory requirements.

In an important Fourth Circuit decision, the court held that an FCA claim may be advanced (under an implied false certification theory) where a government contractor delivers a product or service that does not meet the contractual specifications even if the government contractor neither expressly certified compliance with the contract nor made "specific representations" about the product or service provided. See United States ex rel. Badr v. Triple Canopy, Inc., 857 F.3d 174 (4th Cir. 2017). In that case, the contractor had sought payment for providing security services at an airbase in Iraq. The contract under which the services were provided required the contractor to ensure all employees were qualified on a U.S. Army marksmanship qualification course, but the company's guards were unable to meet the marksmanship requirement – "they couldn't shoot straight." Id. at 175.

The Triple Canopy court held that this alleged misleading omission about the guards' training was the type of "half truth" that can form a false claim under an implied false certification theory of liability. Id. (citing United Health Services v. United States ex rel. Escobar, 136 S.Ct. 1989 (2016)). However, several other circuit courts have interpreted Escobar to require that two conditions be satisfied to state an implied false certification claim: first, the claim for government payment did not merely request payment, but also made specific representations about the goods or services provided; and second, the alleged failure to disclose noncompliance with a material statutory, regulatory, or contractual requirements must make those representations misleading half-truths. See United States ex rel. Rose v. Stephens Institute, 901 F.3d 1124 (9th Cir. 2018); United States v. Sanford-Brown Ltd. , 840 F.3d 445, 447 (7th Cir. 2016). Thus, what is required to assert an implied false certification claim may vary by federal circuit and this can shape the scope of FCA risk for ADG companies.

The standards and qualification requirements imposed by the government are often unique and more onerous than what ADG companies experience in the commercial market. Moreover, noncompliance in the commercial market typically is treated as a contractual action (e.g., breach of contract), but noncompliance in the government market may result in allegations of an FCA violation, which, if successful, could impose significant financial liability and adverse publicity. Consequently, it is especially important for ADG companies to ensure that their contract administration, production, and quality control functions are aligned to ensure compliance with government-imposed unique specifications and quality assurance requirements.

Conclusion

The above-discussion of FCA risk areas suggests those elements of a compliance program that ADG companies will want to prioritize. The compliance program should be reviewed periodically to ensure that it prioritizes the most significant risk areas. These areas currently include; compliance with fast-developing cybersecurity requirements; the delivery of current, accurate, and complete cost and pricing data in the course of negotiating or modifying government contracts; sourcing supplies from "compliant" countries and companies that are not prohibited from providing products or services to government agencies; ensuring accurate and compliant billing; and delivering products and services that meet all applicable quality standards. The risks posed by noncompliance when doing business with the government are typically far greater than those faced in the commercial sector, including from both financial and reputational perspectives. Finally, ADG companies assessing their FCA risk should familiarize themselves with DOJ's new policy for awarding cooperation credit in FCA investigations, which our FCA team summarized earlier this year here.

Michael Mason
Partner
Washington, D.C.

Jonathan Diesenhaus
Partner
Washington, D.C.

Peter Spivack
Partner
Washington, D.C.

Stacy Hadeka
Senior Associate
Washington, D.C.

Michael Scheimer
Senior Associate
Washington, D.C.

Rebecca Umhofer
Knowledge Lawyer
Washington, D.C.

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh*
Rio de Janeiro
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.
Zagreb*

*Our associated offices
Legal Services Center: Berlin

www.hoganlovells.com