Bloomberg Law Reports®

Seller Beware — Caveat Emptor in Reverse in Government Contracting

Claude P. Goddard, Jr., Husch Blackwell Sanders LLP

How candid must a government contractor be with its customer, the U.S. government? Two recent cases suggest that the answer is: disclose all, conceal nothing, and do not exaggerate anything.

In commercial contracting the principle of caveat emptor—buyer beware—prevails. Buyers are expected to see through a seller's puffery and determine for themselves whether the bargain is all it seems to be. In government contracting, however, the rule is different. The seller is held to a high standard of candor as part of its ethical obligations towards the government. This is caveat emptor in reverse—contractors must beware to disclose to the government buyer all facts that could potentially influence the government's decision to award a contract or make a payment.

The obligation of candor in government contracting has long been enforced through a carrot-and-stick approach. The government had available criminal and civil sanctions for false statements or false claims, but it encouraged contractors to report their ethical lapses voluntarily. Recently, however, the government began taking a harsher approach, in part because it perceived contractors were not voluntarily disclosing their misdeeds. The Bush Administration issued regulations[1] in November 2008 mandating that contractors and subcontractors adopt effective ethics and compliance programs and affirmatively come forth to timely report any credible evidence of ethical lapses. Voluntary disclosure became mandatory candor.

The Obama Administration has similarly adopted measures to facilitate the exposure and proof of fraud. In May 2009, President Obama signed into law the Fraud Enforcement and Recovery Act (FERA), which made it easier for the government to prove fraud under the Civil False Claims Act, 31 U.S.C. §§ 3729 *et seq.*, by expanding the range of misrepresentations that are "material" under the Act. Under FERA, any misrepresentation that has the potential to influence any government decision to award a contract or make a payment is actionable under the False Claims Act. This means that contractors will have to be careful not to provide any misleading information to their government customers.

Two recent cases demonstrate just how serious the government is about cracking down on unscrupulous contractors. We examine in this article the circumstances of those cases to show that the government expects contractors to adhere to new, heightened obligations of candor.

The first case, *United States v. BAE Systems plc (BAES)*[2], involved the criminal prosecution of a large defense contractor for conspiring to violate the Foreign Corrupt Practices Act (the FCPA), 15 U.S.C. §§ 78dd-1 *et seq.*, and export control laws and regulations. Although BAES created paper compliance programs and paid lip service to ethical obligations, it actually created an elaborate scheme to circumvent the restrictions of the FCPA and export control laws and cloak its activities in secrecy. That scheme—rather than any underlying FCPA or export control violations—became the focus of the government's prosecution. This case serves as a grim reminder that the cover-up is often a worse offense than the underlying conduct sought to be concealed.

The second case, *United States v. Lithium Power Technologies, Inc.*[3], involved perhaps a more benign scheme to mislead the government. The contractor merely puffed its experience and qualifications to enhance its chances of getting research grants. Nevertheless, its overstatements resulted in both False Claims Act liability and exclusion (debarment) from government contracting for 10 years. This case serves to remind that *any* misrepresentation may lead to fraud proceedings.

The BAES Case

The background to the *BAES* case is set forth in the documents supporting the plea arrangement[4]. BAES, a British company with annual revenues of about $40 billion, is the largest defense contractor in Europe and one of the largest in the United States. In November 2000, as BAES was making a significant expansion into the United States, it made a commitment to the Secretary of Defense that both its U.S. subsidiaries and non-U.S. businesses would operate in full compliance with the FCPA.

The FCPA is an anti-bribery statute that prohibits U.S. companies from making payments to a foreign official to assist in obtaining or retaining business. BAES promised it would adopt compliance programs no later than November 2001 to ensure that BAES affiliates would meet the FCPA anti-bribery provisions.

In 2002, upon hearing rumors that BAES won contracts to supply Eastern European countries with fighter jets by bribing officials, the Department of Defense asked BAES for assurances that the company had lived up to its November 2000 commitments. In mid-2002, BAES confirmed that it had reformed its business practices and had implemented adequate compliance mechanisms to assure that all its businesses were in compliance with the FCPA.

These representations were false. BAES had introduced some compliance policies in 2001, but those were not sufficient to satisfy all of BAES's commitments to the Department of Defense. In actuality, rather than setting up an effective FCPA compliance regime, BAES instead set up elaborate mechanisms designed to conceal the existence of payments to certain "marketing advisors."

BAES employed offshore shell entities to engage and pay certain marketing advisors to assist it in securing sales of defense articles. It also encouraged other of its advisors to establish their own offshore shell entities to receive payments and disguise the origins and recipients of such payments. BAES made payments through

the shell entities, even though there was a high probability that at least part of the payments would be used to ensure that BAES was favored in foreign government decisions concerning sales of defense articles. BAES also avoided communicating with its advisors in writing and failed to maintain adequate information about who its advisors were; what work they were performing; and whether they were performing legitimate activities to justify receipt of substantial payments totaling about $285 million.

BAES also was subject to the Arms Export Control Act (AECA), 22 U.S.C. §§ 2751 *et seq.*, and the U.S. State Department's International Trafficking in Arms Regulations (the ITAR), 27 C.F.R. §§ 120 *et seq.*, which regulate the transfer of U.S. technology on the United States Munitions List. In order to apply for export licenses for Munitions List technology, BAES had to inform the State Department whether it, or any of its vendors, had paid fees or commissions to secure the sale of defense articles.

Despite these obligations, BAES failed to disclose to Sweden or the State Department that it paid commissions totaling about $40 million for assistance in securing the lease by Sweden of Gripen fighter jets to the Czech Republic and Hungary. Because the Gripen fighters contained U.S.-controlled defense materials, Sweden was required to obtain export licenses from the State Department, and BAES, as the licensee, was obligated to disclose to Sweden any commissions relating to the lease. On these facts, the government alleged that BAES engaged in a conspiracy to defraud the United States by causing Sweden to file false applications under the AECA and ITAR.

BAES followed a similar pattern with undisclosed payments for "support services" relating to the sale of Tornado aircraft to the Kingdom of Saudi Arabia. These "support services" were essentially a cover for providing travel and accommodations, security services, real estate, automobiles and personal items totaling over $5 million to a Kingdom of Saudi Arabia official. BAES also used intermediaries and shell entities to conceal payments totaling about $30 million to advisors who assisted in the promotion of this fighter deal. The gain to BAES of all these schemes was over $200 million.

BAES agreed to plead guilty to a Criminal Information[5] charging it with conspiracy to defraud the United States; make false statements to the United States; and violate the AECA and the ITAR by causing the filing of export license applications omitting material facts. The plea deal[6] required BAES to (1) pay a criminal penalty of $400 million; (2) cooperate with the Justice Department; (3) implement an effective compliance system; and (4) retain an independent compliance monitor for three years. BAES entered its guilty plea in the U.S. District Court for the District of Columbia on March 1, 2010, and the Court imposed the agreed sentence.

Lessons from BAES

The obvious points to take from this case are that contractors need to be frank about their compliance efforts and that the cost of shirking ethical obligations is far greater

than the cost of compliance. The $400 million fine imposed on BAES turned a $200 million profit into a $200 million loss.

The collateral fall out within the company was equally dramatic. BAES replaced nearly all of its top leadership, including its Chief Executive Officer and Chairman of the Board, and it severed employment relationships with various members of its senior management who were implicated in the criminal misconduct. It overhauled its compliance organization; retained a new chief legal officer; and it imposed a moratorium on hiring new market advisors and terminated most of its existing ones.

The consequences could have been more severe. BAES's U.S. subsidiaries were not debarred by the U.S. government, but only because the U.S. subsidiaries had no involvement in, or knowledge of, BAES's scheme to avoid the FCPA and export control reporting requirements.

The less obvious lesson is that the issue of whether BAES violated the FCPA became irrelevant to the outcome of the case. The Criminal Information and resulting guilty plea did not depend on proof BAES made illegal payments but, rather, on evidence that BAES schemed to shroud its arrangements with its marketing advisors in secrecy. There was no allegation that BAES violated the FCPA or export control laws. Instead, the government alleged there was a high probability that such payments would be used to assure favorable treatment. The FCPA and export control issues were supplanted by the questions of whether BAES lied about its compliance programs; deliberately avoided learning whether its marketing advisors were violating the law; and concealed information about payments to its advisors. It was the misrepresentations that resulted in the criminal penalty, not an underlying FCPA or export control violation.

The Lithium Power Technologies Case

The second case providing guidance on a contractor's obligation of candor is *Lithium Power Technologies, a 2008 decision*,, in which a small business was held liable for making a false claim based on misrepresentations in research grant proposals. The contractor had to pay triple damages of about $5 million—or three times the entire amount of the grants ($1.6 million). The Air Force also debarred Lithium Power Technologies (LPT) for a period of 10 years—well beyond the normal three year debarment period.

LPT obtained a number of research grants under the federal Small Business Innovation Research (SBIR) Program, which funds research to encourage small companies to develop and commercialize innovative technologies. Under some of its SBIR grants, LPT performed research on the development of lithium batteries for the Air Force, and its research yielded productive results, as it produced batteries that the Air Force found to be satisfactory.

Unfortunately, however, LPT won its SBIR grants dishonestly by engaging in "an elaborate pattern of false statements to secure research grants from the federal government." [7] It portrayed itself in grant applications as a well-established company with extensive facilities that worked cooperatively with prestigious research

institutions. In fact, it was a relatively new company of "dubious qualifications" that likely would not have been selected for SBIR contracts if the government had known the truth.[8]

Companies are selected for SBIR contracts in part based on the qualifications of their research personnel; their facilities and equipment available to perform the research; and the scope of any previously funded work. The Department of Defense does not independently verify all of the information submitted by the applicants but, instead, depends heavily on the integrity of the applicants in providing truthful information.

LPT secured funding under the SBIR program by misrepresenting its:

1. History and status as a SBIR contractor—LPT represented that it was incorporated in 1992 when it had not been founded until 1998;
2. Key personnel available to conduct the research;
3. Physical facilities available to perform the contract—the facilities LPT described were not completed when the SBIR proposals were submitted;
4. Arrangements with research laboratories and academic institutions—LPT falsely stated it had "cooperative research agreements" with the University of Houston and Polyhedron Laboratory when in fact it only paid to use laboratory space at those institutions; and
5. Amount of related work it had performed on prior contracts—it failed to disclose its receipt of prior SBIR contracts when it applied for later Air Force SBIR contracts.

On appeal, one of the principal issues was whether the above misrepresentations were "material" to government decisions to pay LPT for its research work. The Court determined that a misrepresentation was material if it had a natural tendency to influence or was capable of influencing the government's award decision. "All that is required under the test for materiality, therefore, is that the false or fraudulent statements have the potential to influence the government's decisions."[9] Although this case arose before the enactment of FERA, the Court used the same standard adopted in FERA. *Id.*, at 470. In so doing, it rejected more limited materiality standards used by other courts that required a showing that the misrepresentation actually influenced a government decision. *Id.*, at 469–70.

The Court concluded that each of LPT's lies was material. The Court found that LPT's misrepresentation about the existence of cooperative agreements could have misled the Air Force into believing LPT had a formal partnership with those organizations. It found the incorrect incorporation date left the impression that LPT was a much more established and experienced company than it actually was. "In reality, Lithium Power was a company that was in its preliminary stages of development that had yet to demonstrate any proven success."[10]

Lessons from Lithium Power Technologies

This case is a bellwether because, under its (and FERA's) expansive standard of materiality, virtually any exaggeration in an offeror's proposals could be used to prove a False Claims Act violation. For example, many government contracts require

offerors to identify specific persons (often with certain minimum qualifications) who will be available for contract performance. A contractor's later inability to produce those specific individuals could show the contractor misrepresented their availability—just as LPT's misrepresentation of the key personnel available to conduct research was a misrepresentation that, by itself, supported false claims liability.

Similarly, an offeror's failure to identify an organizational conflict of interest would be another type of omission that would have the capability of influencing a selection decision and which would give the government reason to pursue fraud allegations. Such an omission would be analogous to LPT's failure to disclose to the Air Force its prior SBIR work, which supported false claims liability.

In fact, any exaggeration about an offeror's experience or ability to perform a contract could also become the basis for fraud in the inducement allegations—just as LPT exaggerated the facilities it had available to perform the research work and portrayed itself as a more mature operation than it really was. Those exaggerations, by themselves, supported false claims liability.

Finally, it is important to note that LPT's actual performance of the contract became irrelevant. The Court noted the irony of the fact LPT's research yielded useful results, but that finding did not exonerate LPT's misrepresentations. Contractors, accordingly, must expect that, if they are not forthright during the proposal stage, they could be held liable for fraud damages, no matter how well they perform the contract. The most important—and likely only—consideration will be whether the contractor was honest in its proposal.

The New Expectations of Candor

Some clear guidelines can be distilled from the *BAES* and *Lithium Power Technologies* cases to guide contractors in their dealings with the government:

- Compliance obligations are real—they must be taken seriously.
- Contractors must be able to demonstrate that their compliance programs are not just for show—they must actually be effective in detecting and deterring unethical or fraudulent behavior.
- Compliance is required regardless of the contractor's size—BAES is one of the largest government contractors in the world, while LPT is a small business, but they both suffered severe consequences for their ethical lapses.
- Contractors must heed compliance obligations even if they are merely subcontractors—the Federal Acquisition Regulation (FAR) requires that compliance obligations must flow down to subcontractors.
- Contractors must assure they do not misrepresent or overstate their experience, personnel, or qualifications in their proposals—any misstatement could lead to charges the government was fraudulently induced into awarding the contract on the basis of the inaccurate information.
- Contractors cannot expect the government to overlook exaggerations if they perform well—the government will focus solely on the false statement and even exemplary performance will become irrelevant.

- Contractors cannot expect to save money by cutting corners on compliance—even if false claims damages and penalties are disregarded, the costs associated with being investigated, having to defend fraud charges, and potentially losing all government business through debarment will far exceed the costs of implementing effective compliance programs.
- Turning a blind eye to illicit activities of employees or agents is not an effective strategy—contractors can be held liable under the civil False Claims Act if they act with deliberate ignorance or in reckless disregard of the truth.
- A contractor cannot shield itself by keeping innocent intermediaries in the dark—as the *BAES* case shows, contractors can be held liable for failing to disclose facts that render another's statements false.
- Contractors must adapt to the new, heightened expectations of candor—as the *BAES* and *Lithium Power* cases show, the government expects openness, and the FAR requires it.

BAES and *Lithium Power Technologies* represent the wave of the future. In light of those cases and the current compliance climate, the operative mindset now must be "caveat venditor"—seller beware!

*Claude **Goddard** is a partner in the Washington, D.C., office of Husch Blackwell Sanders LLP. Mr. **Goddard**'s legal practice focuses on federal procurement law. He represents clients in corporate internal fraud investigations, false claims actions and agency suspension and debarment proceedings. In addition, he litigates cases involving subcontract issues; misappropriation of trade secrets; government contract claims; bid protests; and default terminations. Mr. **Goddard** frequently writes and lectures on ethics and compliance matters. He may be contacted at claude.**goddard**@huschblackwell.com.*

---

[1] 73 Fed. Reg. 67064 (Nov. 12, 2008).

[2] *United States v. BAE Systems plc*, No. 10-cr-00035, Information (filed D.D.C. Feb. 4, 2010)

[3] *United States v. Lithium Power Technologies*, 530 F. Supp. 2d 888 (S.D. Tex. 2008), aff'd, 575 F.3d 458 (5th Cir. 2009)

[4] The documents are available at http://www.justice.gov/opa/pr/2010/March/10-crm-209.html.

[5] *See* endnote 1.

[6] *BAE Sys. plc*, No. 10-cr-00035, Plea Agreement (D.D.C. Mar. 1, 2010)

[7] *Lithium Power Technologies*, 575 F.3d at 461–62.

[8] *See id.* at 472.

[9] *Id.* at 469.

[10] *Id.* at 472.