New Defense Tech Cos. Must Prioritize Anti-Fraud Compliance

By **Erik Swabb and Elizabeth D'Aunno** (September 9, 2022)

Erik Swabb

Elizabeth D'Aunno

In some ways, the prospects for a technology company entering the defense business have never looked better. Last year saw record global military spending exceeding $2 trillion for the first time, while the U.S. spent $801 billion on the military.[1]

New defense technology companies, such as Anduril Industries Inc.[2] and Epirus Inc.[3], have raised hundreds of millions of dollars at valuations surpassing a billion dollars. They are also starting to win major government contracts.[4]

The war in Ukraine is spurring greater interest in technology with defense applications, such as artificial intelligence,[5] drones[6] and commercial space systems.[7] In June, NATO launched an innovation fund that will invest €1 billion in early-stage startups and other venture capital funds.[8]

That said, defense contracting is not for the fainthearted. Companies face many challenges from the so-called Valley of Death,[9] a term referring to the difficulty of transitioning promising technology from the research-and-development phase into large-scale procurement, to sweeping government data rights claims[10] to other bureaucratic obstacles.[11]

Whether a newcomer is a startup or an established company, it will also need to navigate a legal minefield unlike that found in any other line of business. Littering the minefield are myriad regulations intended to prevent procurement fraud — including bid rigging, bribery, kickbacks, defective and counterfeit products, false billing, and disguising conflicts of interest, among other schemes.

Investing in the compliance resources necessary to adhere to complex rules that mitigate the risk of procurement fraud allegations can be difficult for a company trying to build a fledging defense business. But timely, cost-effective action can help prevent major problems down the road. Too often companies have made shortsighted decisions and paid the price.

Companies weighing investments in compliance can consider procurement fraud risk as a function of impact and probability.

The impact of procurement fraud is straightforward and serious. Procurement fraud implicates a number of laws that carry criminal and civil penalties, and can result in suspension or debarment from current and future government contracts.

The laws prohibiting false claims are among the most important. Submitting a claim for payment to the U.S. government, knowing it to be false, can result in up to five years' imprisonment and fines.[12] Noncriminal false claims also face major penalties.

Under the False Claims Act, for example, a person who fraudulently induces the award of a contract or submits a claim in deliberate ignorance or reckless disregard of its falsity can be liable[13] for three times the amount of the government's damages, plus a penalty[14] for each false claim.

Both prime contractors and subcontractors can face liability for many types of procurement fraud. Moreover, responding to a government inquiry into potential fraud, even if the inquiry ultimately does not establish criminal or civil liability, can be costly for a company — in legal fees, disruption to business operations and reputational damage with key government customers.

The defense sector is arguably the most important, highly regulated and politically sensitive industry in the economy, and these characteristics are mutually reinforcing in ways that raise the probability that companies in this space will come under government scrutiny for potential procurement fraud.

Due to the industry's importance to the nation and the high esteem in which the public holds the U.S. military, the executive branch and Congress are particularly attentive to the activities of defense contractors.

First, there is a heightened risk of noncompliance with statutory and regulatory requirements, generally because the industry is vital to national security. For this reason, the U.S. government has imposed extensive, complex regulatory regimes on defense contractors.

Noncompliance can occur more easily and can carry a higher legal risk than noncompliance with contracts between commercial entities due to, among other things, the prospect of FCA liability arising from a company making express or implied certifications of compliance to the government.

Notwithstanding the U.S. Supreme Court's admonition in its 2016 Universal Health Services Inc. v. U.S. decision that this law is not a "vehicle for punishing garden-variety breaches of contract or regulatory violations,"[15] companies can find themselves involved in protracted government investigations stemming from noncompliance with complex federal contracting requirements.

For example, in October 2021, the U.S. Department of Justice announced its intent to use the FCA to pursue entities for "knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches."[16]

In July, the DOJ announced that Aerojet Rocketdyne Inc. had agreed to pay $9 million to resolve allegations that it violated the FCA by misrepresenting its compliance with cybersecurity requirements in certain federal government contracts.[17]

Second, combating procurement fraud, in particular, is a perennial, bipartisan issue on the Hill and across presidential administrations, and defense contractors should continue to expect acute attention because this is where the government spends most of its contracting dollars.

The U.S. Department of Defense is responsible for about two-thirds of all contracting activity,[18] obligating more than all other federal agencies combined. Moreover, because defense contractor fraud is perceived to tangibly affect national security and the lives of servicemembers, it often draws more media and political attention than contractor misconduct in other sectors.

These dynamics provide powerful incentives for both the executive branch and Congress, whether Democrat or Republican controlled, to dedicate resources to investigating

allegations of procurement fraud by defense contractors, as evidenced by the numerous initiatives both branches have undertaken in recent years.

Executive Branch Initiatives to Detect Procurement Fraud

In November 2019, under the Trump administration, the DOJ announced the formation of the Procurement Collusion Strike Force to target antitrust crimes, such as bid-rigging conspiracies and related fraud.[19] The Biden administration has enthusiastically continued the initiative.

While the strike force is not limited to defense procurement collusion, given that the DOD dominates federal contracting, defense contractors are a prime focus. Most of the indictments and guilty pleas announced by the strike force to date involve defense-related procurements.[20]

This is in addition to the robust civil-fraud enforcement by the DOJ's Civil Division, which since 2012 has recovered close to $1 billion in matters involving defense contracting fraud.[21]

The DOD's Office of Inspector General also devotes significant resources to combating procurement fraud. In 2020, the office reported that roughly one in five ongoing investigations by its Defense Criminal Investigative Service were related to procurement fraud.[22]

The DOD also has a fraud reduction task force that includes subject-matter experts and senior leaders working to reduce fraud risk.[23] Many other DOD entities, such as the Defense Contract Audit Agency, Defense Contract Management Agency and the inspectors general of the military services are well positioned to detect suspected contractor fraud.

Congressional Attention to Defense Procurement Fraud

Congress has paid particular attention to procurement fraud by defense contractors, as well as the DOD's efforts to address it. For the wars in Iraq and Afghanistan, Congress created special inspectors general that reportedly uncovered billions of dollars in fraud, waste, and abuse, and resulted in hundreds of suspensions and debarments.[24]

Some members of Congress are now pushing to establish a special inspector general for the Ukraine war.[25]

In response to congressional requests, the Government Accountability Office conducts audits and reviews of the DOD, and issues reports related to defense contracting fraud.[26] In August 2021, the congressional watchdog reviewed the DOD's fraud risk management, urging action to further address procurement fraud risk.[27]

Third, other features of the defense contracting regulatory regime increase the likelihood of companies coming under scrutiny for procurement fraud absent an investigation initiated by the government.

Under the Federal Acquisition Regulation, government contractors must themselves timely disclose, in writing, credible evidence of violations of certain federal criminal laws or of the civil FCA in connection with the award, performance or closeout of a government contract or subcontracts, or risk suspension or debarment from federal contracting.

Individuals also have strong financial incentives to report suspected procurement fraud. Under the FCA, a private citizen, such as former or current employees and even business competitors, can sue on the government's behalf those who have defrauded the government.[28] If successful, in certain circumstances the plaintiff may receive up to 30% of the amount recovered by the government.[29] Many FCA investigations and lawsuits arise from such qui tam actions.[30]

While the legal and business risk posed by procurement fraud is high, a company can mitigate it by establishing a well-designed compliance program that is adequately resourced and empowered to function effectively.[31] Such programs typically have multiple components, including policies and procedures, employee training, record-keeping, internal reporting channels, and internal auditing and investigations.

Fortunately, companies do not need to reinvent the wheel — they can draw upon government guidance, industry best practices and past matters to implement a cost-effective solution tailored to their particular business needs and regulatory risk profile.

Companies can also benefit from periodic compliance reviews and making preparations to quickly mobilize expertise in government contract investigations in the unfortunate event the company is investigated.

The biggest challenge is often recognizing the need to invest in a procurement fraud compliance program before the company or its employees come under scrutiny for potential misconduct.

Erik Swabb is a partner at WilmerHale and previously served as general counsel of the Senate Armed Services Committee.

Elizabeth D'Aunno is counsel at WilmerHale.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] https://www.sipri.org/media/press-release/2022/world-military-expenditure-passes-2-trillion-first-time.

[2] https://blog.anduril.com/anduril-raises-450-million-in-series-d-funding-671f0a27876b.

[3] https://www.epirusinc.com/news-item/epirus-raises-200-million-in-series-c-funding.

[4] https://www.defense.gov/News/Contracts/Contract/Article/2906241/.

[5] https://www.technologyreview.com/2022/07/07/1055526/why-business-is-booming-for-military-ai-startups/.

[6]https://www.csis.org/analysis/across-drones-ai-and-space-commercial-tech-flexing-military-muscle-ukraine.

[7] https://www.c4isrnet.com/intel-geoint/2022/04/25/how-commercial-space-systems-are-changing-the-conflict-in-ukraine/.

[8] https://www.nato.int/cps/en/natohq/news_197494.htm.

[9] https://www.nationaldefensemagazine.org/articles/2022/1/26/silicon-valley-takes-on-the-valley-of-death.

[10]https://blog.anduril.com/the-dod-should-pilot-a-new-category-of-software-data-rights-a949cc9aaae4.

[11] https://warontherocks.com/2022/04/as-silicon-valley-tries-to-enlist-the-pentagon-strangles-innovation/.

[12] https://www.law.cornell.edu/uscode/text/18/287.

[13] https://www.justice.gov/sites/default/files/civil/legacy/2011/04/22/C-FRAUDS_FCA_Primer.pdf.

[14] https://www.federalregister.gov/documents/2022/05/09/2022-09928/civil-monetary-penalties-inflation-adjustments-for-2022.

[15] Universal Health Servs., Inc. v. United States ex rel. Escobar, 579 U.S. 176, 194 (2016).

[16] https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.

[17] https://www.justice.gov/opa/pr/aerojet-rocketdyne-agrees-pay-9-million-resolve-false-claims-act-allegations-cybersecurity.

[18] https://www.gao.gov/assets/gao-20-106.pdf.

[19] https://www.justice.gov/opa/pr/justice-department-announces-procurement-collusion-strike-force-coordinated-national-response.

[20] https://www.justice.gov/procurement-collusion-strike-force.

[21] https://www.justice.gov/civil/practice-areas-0#defensecontracting.

[22] https://media.defense.gov/2020/Jul/30/2002467835/-1/-1/1/SAR_MAR_2020_BOOK%20V5%20SIGNED_FINAL_20200730_508.PDF.

[23] https://comptroller.defense.gov/Portals/45/Documents/afr/fy2020/DoD_FY20_Agency_Financial_Report.pdf.

[24] https://www.sigar.mil/pdf/special%20projects/SIGAR-21-05-SP.pdf; https://apps.dtic.mil/sti/pdfs/ADA587236.pdf.

[25] https://www.congress.gov/bill/117th-congress/senate-bill/4190/text?r=47&s=1; https://www.congress.gov/bill/117th-congress/house-bill/8094.

[26] https://www.gao.gov/assets/gao-21-309.pdf; https://www.gao.gov/assets/gao-21-104311.pdf; https://www.gao.gov/assets/gao-20-106.pdf.

[27]https://www.gao.gov/assets/gao-21-309.pdf.

[28] https://www.justice.gov/civil/false-claims-act.

[29] https://www.justice.gov/sites/default/files/civil/legacy/2011/04/22/C-FRAUDS_FCA_Primer.pdf.

[30] https://www.justice.gov/civil/false-claims-act.

[31] https://www.justice.gov/criminal-fraud/page/file/937501/download.