BDO USA

ARTICLE

March 27, 2023

The BDO GovCon Week Ahead - March 2023

March 27, 2023

What Is “knowing” under the FCA?

Definition: The False Claims Act (FCA) is an American federal law enacted to take legal action against those persons and companies (often government contractors) who commit fraudulent acts against government agencies and/or government programs. The FCA is also called the “Lincoln law” as the FCA was introduced under the Lincoln administration.

The FCA is the federal government’s primary litigation tool in combatting fraud against the government. For a FCA claim to be successful, one must be able to prove the defendant submitted a false claim or statement “knowingly.” Proving that someone knowingly submitted a false claim or statement is difficult because it is hard to prove what someone knows or does not know.
According to the FCA (31 U.S.C. §§ 3729 – 3733, see 3729(b) Definitions), “knowing” is defined as: “(1) having “actual knowledge of the information;” (2) acting “in deliberate ignorance of the truth or

falsity of the information;" or (3) acting "in reckless disregard of the truth or falsity of the information." By the FCA's definition, a "specific intent to defraud" isn't necessary for someone to be liable for the submission of a false claim or statement.

Companies and persons who do business with the government have expressed and implied duties to familiarize themselves with all applicable, rules, laws, terms, and regulations that apply to their contracts with the government. When a law or regulation is unclear federal agencies will issue further guidance in the form of regulations (agency supplements to Federal Acquisition Regulation for example) or policy announcements. Various court rulings also offer insight into how a law will be interpreted. All of this is helpful if a company or person is trying to determine the correct course of action. However, what happens when there is no authoritative guidance from the government? Can a company be truly "reckless" when it comes to complying with ambiguous regulations or terms? There is an upcoming Supreme Court case, United States ex rel. Schutte v. SuperValu, Inc., that addresses this question. Previously many FCA court decisions have referenced the reasoning in Safeco Insurance Co. of America v. Burr, 551 U.S. 47 (2007) which states essentially that what a defendant thought or believed is irrelevant, as long as their actions were consistent with a reasonable interpretation of an ambiguous requirement.

In conclusion, government contractors should make significant efforts to comply with the terms, laws, and regulations that apply to their contracts. Contractors should also document efforts to be compliant, such as implementation of policies and procedures with effective internal controls that deter non-compliance and training on those controls. In addition, when there is uncertainty, if a contractor seeks help from respectable sources to better understand the law and documents the questions asked and answers received, this could be used in a defense against a "reckless disregard" claim.

For further perspective on what "knowing" means under the FCA please click on the link below:

What Is "Knowing" under the FCA? Supreme Court to Consider Impact of Ambiguous Regulations - Government Contracts Navigator

March 20, 2023

Small Businesses are Entitled for Accelerated Payments in 15 Days – Final Rule Issued by DoD, GSA and NASA

The Department of Defense (DoD), the General Services Administration (GSA), and the National Aeronautics and Space Administration (NASA) issued a final rule on February 14, 2023, to provide for accelerated payments to small business government contractors and subcontractors. The rule, which will be effective from March 16, 2023, requires federal agencies to establish an accelerated payment date to pay small business contractors within 15 days after receiving a proper invoice if the contract does not include a specific payment date or term. In addition, contractors who subcontract with small businesses must make accelerated payments to subcontractors within 15 days after receipt of a proper invoice and (1) a specific payment date is not established by contract; and (2) the contractor agrees to make accelerated payments without further consideration from or fees charged to the subcontractor.

Expected results of this rule include improving the cash flow and access to the Federal marketplace for small businesses. In order to benefit the greatest number of small businesses, the Federal Acquisition Regulatory Council (FAR Council) has determined that the rule will apply to contracts including those at or below the Simplified Acquisition Threshold (SAT) and Commercial Products or Commercial Services, including Commercially Available Off-the-Shelf (COTS) items.

The rule also aligns FAR with Small Businesses Administration (SBA) regulations in several areas including (i) the timing of determination of size status for multiple award contracts; (ii) the implementation of the "ostensible subcontractor rule" as grounds for socioeconomic status protest; (iii) prevention of exercise of options by contracting officers past the fifth year of long term 8(a) contracts if the contractor no longer qualifies for the 8(a) program; and (iv) defining the small business size standard for information technology value added resellers (VARs) under NAICS code 541519 as 150 employees, down from the previous 500 employee standard.

For more information, visit:

- Federal Register / Vol. 88, No. 30 / Tuesday, February 14, 2023 / Rules and Regulations
- Federal Acquisition Regulation: Accelerated Payments Applicable to Contracts With Certain Small Business Concerns

March 13, 2023

GAO Protest Highlights the Importance of Compliance and Burden of Proof

In the world of government contracting, the selection of a contractor who has employed ex-agency personnel might raise doubts about potential organizational conflicts of interest (OCI) because such individuals may be privy to private information that may provide a competitive advantage. However a decision by the Government Accounting Office (GAO) in a recent bid protest highlights how difficult it may be for a protester to show this advantage.

In B-420881 Cybermedia Technologies, Cybermedia challenged the award of a task order by the Department of Defense Counterintelligence and Security Agency (DCSA) to The Prospective Group alleging that DCSA failed to assess and mitigate an OCI arising from the awardee's principal subcontractor which had hired five former agency officials. Cybermedia asserted that the individuals provided Prospective with access to competitively useful information that provided Prospective an unfair advantage. DCSA asserted that four of the five individuals left the agency prior to the start of planning of the request for proposal (RFP) for the task order and that the fifth individual was hired by the subcontractor after Cybermedia and Prospective had submitted their proposals. The GAO in its decision found that the protester had furnished only unfounded suspicions about unspecified proprietary information and that "hard facts", not speculation, must be present to show an unfair advantage. These facts must include whether an individual had access to non-public information that was not available to other firms and whether the information was competitively useful.

In summary, protesters must provide concrete evidence to show that the contractor has an actual or potential conflict of interest that would prevent it from providing impartial advice or services. This can be a difficult standard to meet but is essential to ensure fair competition in government contracting. Please access GAO's decision below for more information.

March 6, 2023

An Evolving Cybersecurity Landscape Sparks Changes to Guidance

The National Institute of Standards and Technology (NIST) Cybersecurity Framework ("CSF" or "Framework") was developed in 2014, and later updated in 2018, in response to increased cybersecurity risk to the nation's critical infrastructure. Once again, NIST is seeing the need to modify the framework to combat the most prevalent cyber risks and is adding another pillar of guidance to create CSF 2.0.

NIST plans to add “Govern” to the current framework that already features Identify, Protect, Detect, Respond, and Recover. Govern will be a cross-sectional pillar that informs the other framework sections about the evaluation of cybersecurity risk, determination of cybersecurity roles and responsibilities, and establishment of cybersecurity policies and procedures. The update aims to emphasize the importance of risk management and continuous monitoring of regulatory requirements within your organization.

In this update NIST identifies a “Call to Action” singling out ways in which the community can contribute to improvements to CSF 2.0 and associated resources:

1. Share International Resources
2. Provide Mappings
3. Share additional example profiles for specific sectors, threats, and use cases,
4. Submit CSF Resources - These can include approaches, implementation guides, mappings, case studies, tools, and others.
5. Share Success Stories
6. Share Use of the CSF in Measuring and Assessing Cybersecurity
7. Comment on Performance Measurement Guide for Information Security

In addition to the change in framework structure, CSF 2.0 will include additional guidance on supply chain management risk and impact. Contractors whose supply chain operations utilize third-party organizations, outsourcing, and new supply chain technology will be expected to enhance risk assessment strategy that could include the implementation, or appointment, of a team to mitigate that risk.

Among the already discussed updates, NIST plans to:

- Keep guidance broad so that it does not limit the application across sector, industry, business line.
- Provide contractors examples for ways in which the framework could be implemented.
- Provide additional resources that help contractors measure cybersecurity risk. This will include ways that other contractors have performed assessment and mitigation.

Although the CSF 2.0 has not been finalized, it has garnered a positive response throughout the cybersecurity community and should be on your organizations' radar.