PUBLICATION

Failure to Comply with the Cybersecurity Requirements of Your Government Contracts Can Lead to False Claims Act Liability

September 2019

Two recent cases now prove that to avoid liability under the False Claims Act (FCA), government contractors must build and monitor information systems to protect government information and must also implement policies and procedures that comply with applicable requirements.

For government contractors who have attended Baker Donelson's recent presentations about significant FAR and DFARS updates, you know that we have been warning for several months that the failure to comply with cybersecurity requirements in your government contracts could lead to significant FCA liability. This is especially true for defense contractors who certify cybersecurity compliance by submitting an offer in response to a solicitation that contains DFARS 252.204-7008 – *Compliance with Safeguarding Covered Defense Information Controls (Oct. 2016)*. The cases discussed in this alert show that the risk of cybersecurity noncompliance is significant.

Significant False Claims Act Settlement Based on Alleged Cybersecurity Failures

On July 31, 2019, an $8.6 million FCA settlement was announced and the qui tam[1] complaint was unsealed in the matter of *United States, et. al., ex. rel. James Glenn v. Cisco Systems, Inc.*,[2] which resolved allegations that a government contractor sold video surveillance manager software (VSM) to federal, state, and local government agencies when it knew that the software allowed unauthorized access to government information.

In *ex. rel. James Glenn*, the qui tam relator, James Glenn, discovered that the VSM software had several security flaws that allowed a person with even moderate knowledge to access all video feeds, user passwords, and all stored data in the system and allowed unauthorized persons to modify or delete video feeds. The complaint alleged that these collective flaws would allow an unauthorized user to "effectively shut down an entire airport by taking control of all security cameras and shutting them off" or to "access video archives of a large entity to obscure or eliminate video evidence of theft or espionage."[3]

The complaint claimed that Glenn reported these flaws to his employer on multiple occasions between October 2008 and March 3, 2009, but the issues were not resolved. Without warning, on March 9, 2009, Glenn's employment was terminated. After his termination and after reporting the issues to the FBI, Glenn then proceeded to file his FCA qui tam complaint on May 10, 2011. After several years of litigation, on July 31, 2019, it was announced that the entire case was resolved for $8.6 million. The settlement is considered a landmark ruling as it is the first significant FCA settlement based on the failure to comply with cybersecurity requirements.

District Court Refused to Dismiss Complaint Alleging Cybersecurity Noncompliance

Earlier this summer in a case based on similar allegations, the Eastern District of California refused to dismiss FCA claims in *United States ex rel. Markus v. Aerojet Rocketdyne Holdings* (*ex. rel. Markus*), where the relator alleged that his employer repeatedly made false certifications to the government about compliance with DFARS clauses related to cybersecurity.[4] The relator, Brian Markus, was the Senior Director of Cyber Security, Compliance, and Controls for a missile defense and rocket engine technology company that holds contracts with the Department of Defense (DoD) and NASA.

Markus filed an FCA qui tam action on behalf of the United States alleging that his employer did not comply with applicable DoD and NASA cybersecurity regulations, and repeatedly made misrepresentations to the government about its compliance. After the government refused to intervene, Markus' employer filed a Motion to Dismiss asserting that the alleged noncompliance was not material to the government because the government knew about the noncompliance and still made payments for the goods and services with full knowledge of the noncompliance. A falsehood is only material under the FCA if it has "a natural tendency to influence, or be capable of influencing, the payment or receipt of money or property."[5]

The court in *ex. rel. Markus* refused to dismiss the case and held that the alleged misrepresentations were material because, although the contractor disclosed certain areas of noncompliance, it allegedly failed to disclose the full extent of its noncompliance. The court also noted that even if the government awards a contract knowing that a contractor has areas in which it is not fully compliant, that does not mean that the contractor can rely on the government's knowledge and acceptance of partial compliance to then proceed with performance without ever becoming entirely compliant.[6] Therefore, if the clause is in the contract, like all other requirements, the contractor needs to comply with it. If there are areas where contractors are still working towards compliance, those should be accurately and fully disclosed.

Impacts on Government Contractors

The FAR Council and several government agencies have made several regulatory updates in recent years to directly address cybersecurity. For example, FAR 52.204-21 – *Basic Safeguarding of Covered Contractor Information Systems* became effective in June 2016 and requires contractors to implement several "basic" information security requirements. Defense contractors whose information systems process, store, or transmit "covered defense information" must also comply with DFARS 252.204-7012 – *Safeguarding Covered Defense Information and Cyber Incident Reporting*. To be compliant with DFARS 252.204-7012, since December 31, 2017, defense contractors have been required to implement the controls and policies that are set out in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 standards. Significantly, any defense contractor that submits a proposal in response to a solicitation that contains DFARS 252.204-7008 certifies compliance with the NIST SP 800-171 standards, which directly implicates the FCA discussion above. Several other government agencies also have announced their intentions to increase cybersecurity requirements for government contractors.

As shown by the above cases and the several recent regulatory changes, the government is serious about cybersecurity and expects its contractors to follow suit. The Government Accountability Office (GAO) reported that *government agencies faced 35,000 cyber incidents in FY 2017 alone*. Contractors need to take steps to ensure their cyber systems protect government information. Taking such steps will, in turn, provide greater protection for the contractor to avoid FCA liability related to cyber requirements. Some practical basic steps that should now be taken by government contractors include the following.

- Review your government contracts to evaluate the cybersecurity clauses that are incorporated, including FAR 52.204-21, DFARS 252.204-7008, and DFARS 252.204-7012. Make sure you fully understand your security obligations.

- Coordinate with internal information technology personnel to audit cybersecurity controls and policies to ensure compliance with the NIST SP 800-171 standards to the extent that your government contract requires NIST compliance. Contractors should note that NIST SP 800-171 standards require the implementation of both technology solutions and policies and procedures to achieve full compliance.

- Incorporate cybersecurity policies into your Code of Business Conduct and Ethics Policy to create a culture of compliance related to these issues. Employees should be trained on how their own use of

technology can damage the entire organization. Employees also should have a hotline or contact where they can report any cyber incidents or compliance issues immediately after they are identified.

- Be aware of the significance of the government's cybersecurity clauses, and fully and accurately explain your compliance with cyber requirements to the government in all communications on the subject. Government contractors would be wise to involve legal counsel in both reviewing proposals before they are submitted and in communicating about any compliance issues. To the extent that you identify any potential issues with cybersecurity compliance, talk with your government contracts attorneys so those issues can be fully addressed by legal professionals who have your best interests in mind.

Baker Donelson's Government Contracts Team routinely assists contractors with acquisition regulation compliance, and with communications with the government after compliance issues arise. Baker Donelson's Data Protection, Privacy, and Cybersecurity Team also routinely assists organizations with privacy and cybersecurity diligence and risk assessments. For more information on these topics, please contact your existing Baker Donelson attorney.

[1] 31 U.S.C. §§ 3279 et seq. The qui tam provision at 31 U.S.C. § 3730(b) allows individuals to file an FCA complaint on behalf of the government. The complaint must be filed under seal and served on the U.S. Attorney for the district where the case is filed and on the Attorney General of the United States.

[2] *United States, et. al., ex. rel. James Glenn v. Cisco Systems, Inc.*, Case No. 1:11-cv-00400-RJA, Doc. No. 75 (W.D.N.Y. July 31, 2019).

[3] *Id.,* Doc. No. 1, Compl. ¶ 64 (May 10, 2011).

[4] *United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc., and Aerojet Rocketdyne, Inc.*, Doc. No. 57, 2:15-cv-02245 (E.D. Cal. May 8, 2019).

[5] 31 U.S.C. § 3729(b)(4).

[6] *United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc., and Aerojet Rocketdyne, Inc.*, Doc. No. 57, 2:15-cv-02245, at p. 9 of 17 (E.D. Cal. May 8, 2019).