Published on *The National Law Review* https://natlawreview.com

Defense Contractor Denied FCA Summary Judgment in First Test of DOJ's New Civil Cyber-Fraud Initiative

Article By:

Brad Robertson

Daniel J. Fortune

Ocasha O. Musah

On February 1, 2022, the United States District Court for the Eastern District of California ruled that a False Claims Act (FCA) case against defense contractor Aerojet Rocketdyne Holdings and Aerojet Rockdyne Inc. (collectively "Aerojet") could go forward on triable issues of fact as to whether noncompliance with government cybersecurity requirements are material to the government's decisions to approve contracts. The federal court denied Aerojet's motion for summary judgment and issued the first major ruling in an FCA case testing the Department of Justice's new Civil Cyber-Fraud Initiative.

Announced in October 2021, the purpose of the government's Civil Cyber-Fraud Initiative is to utilize the FCA to pursue cybersecurity-related fraud by government contractors and grant recipients. DOJ announced plans to focus on entities that knowingly misrepresent their cybersecurity practices or protocols, knowingly violate obligations to monitor and report cybersecurity incidents and breaches, or knowingly provide deficient cybersecurity products or services. In this case, the relator — the defendant's former senior director of Cybersecurity, Compliance & Controls — alleged that Aerojet knew its cybersecurity programs fell short of Department of Defense and NASA acquisition regulations, which were part of contracts between Aerojet and the agencies.

Despite declining to intervene in the Aerojet case in June 2018, the government filed a statement of interest two weeks after it announced the Civil Cyber-Fraud Initiative, assailing Aerojet's arguments that it was entitled to summary judgement. Notably, the government argued that the contractual deficiencies were a source of damages even if Aerojet otherwise complied with the contracts because "the government did not just contract for rocket engines, but also contracted with [Aerojet] to store the government's technical data on a computer system that met certain cybersecurity requirements." The government also argued that assertions that the entire defense industry is not compliant with cybersecurity requirements has no bearing on whether such compliance is material to the government's payment decision in any particular case.

The court commented on how the relevant regulations required government contractors to implement

specific safeguards to protect unclassified technical information from cybersecurity threats. Although the court acknowledged that Aerojet may have disclosed certain cybersecurity shortcomings to the government, the court questioned whether Aerojet failed to disclose key events, and the results of audits showing gaps in Aerojet's cybersecurity. The court also expressed concern as to whether Aerojet knowingly misrepresented their intention to comply with the cybersecurity provisions of their contracts in the first place. Given the new initiative, the filing of the statement of interest in this case, and this recent federal ruling, government contractors and grant recipients would be wise to review the cybersecurity requirements in their contracts, grants, and licenses to ensure compliance and avoid being caught in the snare of the government's new focus on cybersecurity.

National Law Review, Volume XII, Number 39