Akin®

DOJ's Cyber Review and Aerojet $9 Million Settlement Signal Continuing FCA Enforcement for Cybersecurity Violations by Government Contractors

Jul 22, 2022

Reading Time : **2 min**

By: Natasha G. Kohne, Marta A. Thompson

The Review also noted that where contractual cybersecurity standards were not met, the Department's Civil Cyber-Fraud Initiative (CCFI) would continue to utilize the False Claims Act (FCA) to pursue cybersecurity-related fraud by government contractors and grant recipients. The CCFI was first announced in October 2021. The Review comes on the heels of a recent FCA settlement with Aerojet Rocketdyne Inc. for alleged fraudulent misrepresentations of compliance with cybersecurity standards.

On July 8, 2022, the Department announced that Aerojet 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 and subcontracts. Aerojet, based in El Segundo, California, provides propulsion and power systems for launch vehicles, missiles and satellites, and other space vehicles to the Department of Defense (DOD), the National Aeronautics and Space Administration (NASA) and other federal agencies. Those contracts are subject to the Federal Acquisition Regulation (FAR) and agency-specific supplements to the FAR, such as the Defense FAR Supplement (DFARS) and NASA FAR Supplement (NASA FARS), which in part require compliance with cybersecurity standards around safeguarding covered defense and sensitive unclassified information, and cyber incident reporting.

The settlement resolves a lawsuit filed by a former Aerojet employee against the company under the *qui tam*, or "whistleblower," provisions of the FCA, which authorize a private party to file suit and litigate FCA claims on behalf of the federal government in exchange for a

portion of any recovery. The whistleblower, who previously served as the Senior Director of Cyber Security, Compliance & Controls, alleged that Aerojet had entered into multiple federal contracts and subcontracts that required compliance with cybersecurity standards such as DFARS clause 252.704-7012 (which incorporates National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171) and NASA FARS clause 1852.204-76, despite the company's knowledge that its systems did not meet those requirements.

The Review and the Aerojet settlement signal an ever-increasing focus by the Department and sponsor agencies on contractor and grantee compliance with cybersecurity regulatory requirements, and may further invite whistleblower actions as well.

The *qui tam* case is *United States ex rel. Brian Markus v. Aerojet Rocketdyne Holdings Inc., et al.*, Case No. 2:15-cv-02245-WBS-AC (E.D. Cal.).

Categories

Corporate Governance

Cybersecurity, Privacy & Data Protection

Cybersecurity & Information Security

Federal Privacy Policy

Government Contracts

Subscribe to the Data Dive Blog Series >