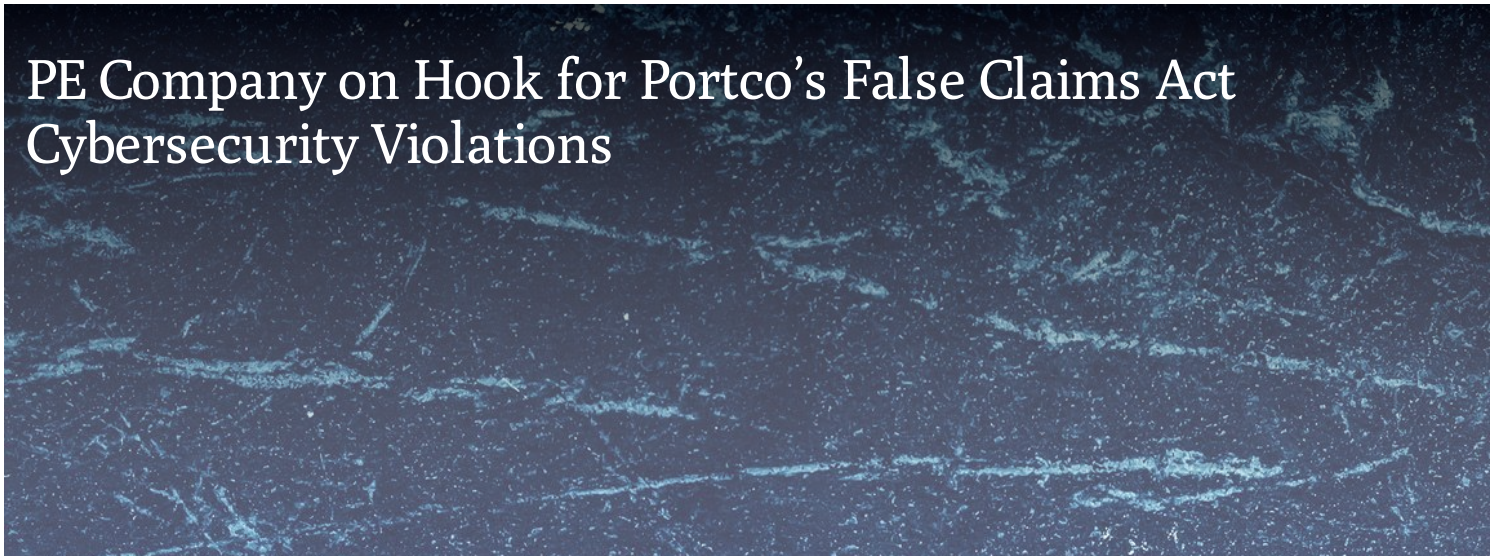
WINSTON & STRAWN LLP

BLOG

PE Company on Hook for Portco's False Claims Act Cybersecurity Violations



AUGUST 18, 2025

DOJ False Claims Act (FCA) settlements related to cybersecurity typically have focused on false representations by a government contractor of its compliance with cybersecurity requirements. A recently announced settlement shows that private equity owners are not immune from potential FCA liability. A private equity owner, Gallant Capital Partners LLC (Gallant) of Aero Turbine Inc. (ATI), a government contractor in Gallant's portfolio, recently agreed to pay the U.S. government $1.75 million to settle claims under the civil False Claims Act (FCA) concerning ATI's alleged failure to meet cybersecurity requirements under a U.S. Air Force contract. ATI is an aerospace maintenance, repair, and overhaul service provider that contracted to repair and maintain J85 turbojet engines for the Air Force.

The settlement did not arise from a qui tam whistleblower, ut rather Gallant and ATI disclosed to the government ATI's noncompliance with cybersecurity requirements relating to the Air Force contract. Neither ATI nor Gallant admitted FCA liability, and both cooperated with the government's investigation by identifying individuals involved in or responsible for the alleged noncompliance. Gallant's potential FCA liability flowed directly from its majority ownership of ATI. The settlement resolves allegations under the FCA that ATI did not fully implement necessary security controls, risking exposure to controlled defense information, while it submitted invoices to the government for payment under the Air Force contract.

Specifically, the government alleged that ATI and Gallant failed to control confidential unclassified information (CUI) and limit access to the information system used under the contract to only authorized users. The company apparently allowed a software company with personnel in Egypt to access the information system and its data, which included CUI related to the Air Force contract.

The Air Force contract at issue incorporated Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, which requires Department of Defense (DoD) contractors and subcontractors to provide adequate security on all covered contractor information systems to safeguard covered defense information by, at a minimum, implementing the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations." Apparently, although ATI assumed its cybersecurity controls were sufficient to meet its cybersecurity obligations under the Air Force contract, ATI failed to verify whether it met the specific cybersecurity controls in NIST SP 800-171.

In announcing the FCA settlement, the government stated that "[t]his case serves as a reminder that cybersecurity transcends mission sets" and it will ensure that "companies adhere to robust cybersecurity requirements," which are integral to maintaining the government's "operational edge against adversaries." The government hailed this FCA settlement as a warning that "[e]very defense contractor must provide adequate security to safeguard covered defense information."

KEY TAKEAWAYS:

- PE firms can be exposed to FCA liability based on material noncompliance by their portfolio companies.
- PE firms must perform careful due diligence during the acquisition process to ensure that portfolio companies holding federal contracts have adhered to, and will continue to comply with, government cybersecurity compliance requirements, especially in the defense sector.
- After closing, and on an ongoing basis, PE firms should understand and engage counsel to assess their portco's compliance with the Federal Acquisition Regulation and DFARS requirements, including cybersecurity requirements specified in the government contracts.

Winston's Washington, D.C. based Government Contracts & Grants Team regularly assists in specialized due diligence in PE and M&A transactions, including, among others, diligence related to a contractor's cybersecurity compliance obligations, and provides counseling to portfolio companies to ensure compliance with the FAR and DFAR.

2 Min Read

Authors

Lawrence S. Sher

Elizabeth Leavy

Lawrence "Larry" Block

William T. Kirkwood

Related Topics

False Claims Act (FCA) | Cybersecurity | Department of Justice (DOJ) | Private Equity | Defense

Related Capabilities

White Collar & Government Investigations

Government Program Fraud, False Claims Act & Qui Tam Litigation

Government Contracts & Grants

Related Professionals

Lawrence S. Sher

Elizabeth Leavy

Lawrence “Larry” Block

William T. Kirkwood

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.