WINSTON & STRAWN LLP

BLOG

DOJ Civil Cyber-Fraud Initiative Continues to Impact Government Contractors – The Latest False Claims Act Settlement

OCTOBER 24, 2024

On October 22, 2024, the Department of Justice announced a False Claims Act (FCA) settlement related to a government contractor's failure to adhere to certain cybersecurity requirements. Specifically, Pennsylvania State University (Penn State) has agreed to pay US$1.25M to resolve allegations that it violated the FCA by failing to comply with cybersecurity requirements in fifteen contracts or subcontracts involving the Department of Defense (DOD) or the National Aeronautics and Space Administration (NASA). The DOJ announcement is available here: https://www.justice.gov/opa/pr/pennsylvania-state-university-agrees-pay-125m-resolve-false-claims-act-allegations-relating.

In October 2021, the DOJ established the Civil Cyber-Fraud Initiative to "utilize the False Claims Act to pursue cybersecurity related fraud by government contractors and grant recipients." According to the DOJ, the initiative would "hold accountable entities or individuals that put U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches." https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative?utm_medium=email&utm_source=govdelivery.

This FCA settlement continues a trend of FCA settlements related to cybersecurity, including the following examples:

- July 8, 2022 settlement for US$9M by Aerojet to resolve allegations that it violated the FCA by misrepresenting its compliance with cybersecurity requirements in certain federal government contracts and subcontracts.
- March 14, 2023 settlement for $293,771 by Jelly Bean Communications Design LLC to resolve allegations that it violated the FCA related to a failure to secure personally identifiable information (PII).
- May 1, 2024 settlement for US$2.7M by Insight Global LLC to resolve allegations that it violated the FCA by having deficiencies in cybersecurity measures in performing a pandemic-related government contract.
- October 15, 2024 settlement for $306,722 and waiver of a claim of at least $877,578 by ASRC Federal Data Solutions LLC to resolve allegations that it violated the FCA by failing to properly protect PII resulting in a data breach.

Another FCA case is pending against the Georgia Institute of Technology (Georgia Tech) and its Board of Directors, alleging that the university failed to meet certain cybersecurity requirements in its performance of DOD contracts. DOJ alleges that Georgia Tech failed to implement contractual cybersecurity controls required by DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, under contracts with the U.S. Air Force and the Defense Advanced Research Projects Agency (DARPA). DOJ further alleged that the university "intentionally, knowingly, and negligently" provided DOD a false campuswide summary level score under DFARS 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements, rather than a score for the information technology systems where research involving covered information was actually conducted, with "the intention of inducing DoD to award and retain government contracts[.]" The defendants in that case recently filed a motion to dismiss.

In addition to the FCA cases that DOJ is pursuing for false certifications and representations related to cybersecurity, cybersecurity currently is a major focus for government contractors, as the government recently issued a Final Rule for the Cybersecurity Maturity Model Certification (CMMC) Program. As stated in the Final Rule's announcement: "The purpose of CMMC is to verify that defense contractors are compliant with existing protections for federal contract information (FCI) and controlled unclassified information (CUI) and are protecting that information at a level commensurate with the risk from cybersecurity threats, including advanced persistent threats."

https://www.defense.gov/News/Releases/Release/Article/3932947/cybersecurity-maturity-model-certification-program-final-rule-published/.

As cybersecurity rules change, government contractors need to keep informed and ensure they are compliant with the changed rules and that any certifications/representations in their prime or subcontracts are informed and correct.

TAKEAWAYS:

1. The DOJ continues to enforce cybersecurity requirements in government contracts and is extracting large settlements. Compliance is no longer an abstract concept. Failure to adhere to cybersecurity requirements may result in significant FCA liability and potential suspension/debarment.
2. Small, medium, and large government contractors need to take cybersecurity requirements seriously and implement a comprehensive plan for timely compliance. Government contractors must review all active government contracts to assess if their contracts include cybersecurity requirements and if so, whether or not the company is in compliance. If not in compliance, each invoice submitted to the government under the contract can be an implied false certification, exposing the company to liability under the FCA.
3. Subcontractors need to be aware of cybersecurity flowdown obligations because FCA liability is applicable to subcontractors as well for any false certifications or representations, either express or implied, related to cybersecurity requirements.

Winston & Strawn's Government Contracts & Grants Practice is a nationally recognized, highly regarded group of lawyers with deep experience in handling FCA matters and high-value, and often contentious, government contract disputes, bid protests, and claims across a broad spectrum of industries and issues.

Please contact our Winston Government Contracts & Grants team if you have questions about this initiative or its implications for your business: Lawrence Block, Lawrence Sher, Elizabeth Leavy, William Kirkwood, and Frank DiNicola.

4 Min Read

Authors

Lawrence "Larry" Block

Lawrence S. Sher

Elizabeth Leavy

William T. Kirkwood

Frank V. DiNicola

Related Topics

FCA | DOJ | Cyber Security | Compliance

Related Capabilities

Government Investigations, Enforcement & Compliance

Government Program Fraud, False Claims Act & Qui Tam Litigation

Government Contracts & Grants

Related Professionals

Lawrence “Larry” Block

Lawrence S. Sher

Elizabeth Leavy

William T. Kirkwood

Frank V. DiNicola

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.

© 2024 Winston & Strawn LLP.