GT GreenbergTraurig

Alert | Government Contracts

August 2024

DOJ Files Complaint in First Cybersecurity False Claims Act Qui Tam Case Intervention

Go-To Guide:

- On Aug. 22, 2024, the Department of Justice filed its complaint-in-intervention against the Georgia Tech Research Corporation and the Georgia Institute of Technology, raising claims under the False Claims Act (FCA) and federal common law. This is the first FCA lawsuit the United States has intervened in as part of DOJ's Civil Cyber-Fraud Initiative.
- DOJ's lawsuit comes just four months after it intervened in the relator FCA action brought in July 2022 by two whistleblowers, alleging the defendants failed to comply with NIST 800-171 cybersecurity controls and other requirements in their Department of Defense contracts.
- DOJ has now added its own allegations that the defendants failed to meet cybersecurity requirements in their DoD contracts and misrepresented their self-assessment score.
- DOJ's allegations highlight the importance of contractors and subcontractors verifying their security assessments. Under the Cybersecurity Maturity Model Certification (CMMC) proposed rule issued earlier this month, DoD contractors will report their confidence level in their security assessment scores or provide annual affirmations.

In July 2022, two relators sued the Georgia Tech Research Corporation (GTRC) and the Georgia Institute of Technology (GA Tech) under the FCA. The allegations include violations of the FCA and employment law, based on the "increasing retaliation" experienced by the relators after they escalated their concerns. In February 2024, the DOJ intervened in the case, and on Aug. 22, 2024, with the U.S. Attorney's Office for the Northern District of Georgia, DOJ filed its complaint-in-intervention (Complaint), raising its own allegations under the FCA and federal common law alleging that GTRC and GA Tech failed to meet cybersecurity requirements in connection with the performance of their DoD contracts. This is the first FCA litigation matter where the DOJ has intervened as part of the Civil Cyber-Fraud Initiative.

Overview of DFARS Cybersecurity Provisions

Since 2013 contractors and subcontractors have been required to provide "adequate security" to protect controlled unclassified information (CUI) that resides on a covered contractor information system. *See* DFARS 252.204-7012. Since 2016 "adequate security" has entailed compliance with the version of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 in effect at the time a solicitation is issued. *Id*. Contractors should have a Plan of Action and Milestones (POAM) for each control that is not fully implemented. The contract clauses also state that by submitting their offers, contractors are representing that they will implement the NIST SP 800-171 controls. *See* DFARS 252.204-7008(c)(1). In December 2020, additional clauses were issued providing for an assessment against the NIST SP 800-171 controls, which should be filed in the Supplier Performance Risk Management System (SPRS). *See* DFARS 252.204-7019. The score, the scope of assessment, and the date by which the contractor intends to implement the NIST SP 800-171 controls must be posted at the time of contract award for each covered contractor information system that is relevant to the contract.

Key Allegations of Cybersecurity Violations

DOJ's allegations focus on one lab at GA Tech, the Astrolavos Lab, and two contracts that lab held between 2016 and the present. DOJ alleges that these contracts incorporated the requirements to comply with NIST SP 800-171, and the later-in-time contract incorporated the self-assessment requirements. According to DOJ, testimony from GA Tech's staff indicates that both contracts also included CUI. The allegations focus on three main areas of noncompliance: the failure to have in place a comprehensive System Security Plan (SSP) in accordance with NIST control 3.13.4; the failure to install, update, and run antivirus software in accordance with NIST control 3.14.2; and the failure to post an accurate NIST self-assessment score.

- NIST control 3.12.4 directs contractors to "[d]evelop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems." DOJ alleges that Astrolavos Lab failed to have an SSP until February 2020 and that the SSP which was developed was limited to servers, rather than encompassing the laptops and desktops that would also hold CUI. The lab developed another SSP in August 2023 for a separate contract, but that was nearly a year after CUI was incorporated into the contract and was also inadequate because it did not fully address all covered systems.
- NIST control 3.14.2 directs contractors to install antivirus software throughout an IT environment, including on hosts such as workstations, servers, mobile devices, firewalls, email servers, web servers, and remote access servers. DOJ alleges that Astrolavos Lab failed to install, update, and run antivirus software from at least 2016 until December 2021.

- DOJ also alleged that the assessment score posted in SPRS was inaccurate because the scope of the assessment was not properly identified.

DOJ alleges that staff at GA Tech were aware of the above issues and the regulatory requirements imposed on GA Tech, and that the violations were material to payment decisions by the government for the following reasons:

- Cybersecurity is critical to national defense, quoting from multiple executive orders issued by Presidents Obama, Trump, and Biden, as well as DoD policies and guidance.

- Cybersecurity compliance is a condition of contract, and therefore a condition of payment. DOJ notes that GA Tech was sent a cure notice under one of the contracts based on the alleged violations of the cybersecurity requirements.

Key Takeaways for Contractors

The intervention and allegations in the Complaint demonstrate DOJ's continued focus on cybersecurity fraud and enforcing contractor compliance with cybersecurity requirements under the Civil Cyber-Fraud Initiative. In announcing the Complaint, DOJ also highlighted the risk that deficiencies in cybersecurity pose to our national security and the safety of our armed services, stating that "government contractors that fail to fully implement required cybersecurity controls jeopardize the confidentiality of sensitive government information" and the goal is "to identify such contractors and to hold them accountable."

DOJ's actions here align with DoD's rulemaking activities on CMMC, which propose more robust controls around contractor verification of cybersecurity control implementation. Contractors should carefully review any requests for verification or attestations related to cybersecurity compliance. For example, under the new proposed rule contractors and subcontractors may need to provide a confidence level in their assessment or provide an annual affirmation of their assessment. Contractors should be alert to any such requirements and the increased risks such statements may impose.

Contractors must also keep in mind that cybersecurity obligations have been part of DoD contracts and subcontracts since at least December 2017. This case emphasizes that DoD contractors and subcontractors at all tiers risk significant consequences if they fail to meet cybersecurity compliance obligations. Contractors should carefully review their existing contracts and clarify any questions regarding the application of any cybersecurity requirements, as well as verify the accuracy of any explicit or implied statements of compliance.

Authors

This GT Alert was prepared by:

- Eleanor M. Ross | +1 202.530.8565 | Eleanor.Ross@gtlaw.com
- Cassidy Kim | +1 415.590.5133 | Cassidy.Kim@gtlaw.com
- Jeffery M. Chiow | +1 202.331.3149 | Jeff.Chiow@gtlaw.com

Sacramento. Salt Lake City. San Diego. San Francisco. Seoul.∞ Shanghai. Silicon Valley. Singapore.⁼ Tallahassee. Tampa. Tel Aviv.^ Tokyo.¤ United Arab Emirates.‹ Warsaw.~ Washington, D.C.. West Palm Beach. Westchester County.