DORSEY
DORSEY+WHITNEY LLP

DOJ on Campus: DOJ's First Intervention in False Claims Act Case Alleging University Knowingly Failed to Meet Contractual Cybersecurity Requirements

by Nicole Engisch, Alex Hontos, and Seth Goertz

Cybersecurity requirements for federal contractors and grantees continue to proliferate—and those requirements do not just come with contractual risk. Increasingly, the United States government is leveraging enforcement tools, particularly the False Claims Act (and its treble damages), to police these requirements. A recent action against a public research institution is a good case study for compliance officers and legal professionals who advise recipients of federal funding.

The United States Department of Justice (DOJ) recently announced that it had intervened in a whistleblower's False Claims Act case against the Georgia Institute of Technology and Georgia Tech Research Corp., a non-profit contracting entity for Georgia Tech (GTRC). The complaint-in-intervention alleges that these entities (collectively, Georgia Tech) knowingly failed to meet contractual cybersecurity requirements in performance of Department of Defense (DoD) contracts.[1] The original whistleblower lawsuit was filed months earlier by a current and a former member of Georgia Tech's cybersecurity compliance team.

As the complaint explains, defense contractors typically must comply with DoD contractual cybersecurity requirements to protect any non-public government information that can be accessed from contractors' information systems. [2] DoD imposes cybersecurity requirements to minimize threats to national security and the U.S. economy from malicious cyber activity and theft of intellectual property. The federal government has specifically warned research universities that they are known targets for cyberattacks by foreign intelligence services and other foreign adversaries.

From as early as 2019, Georgia Tech allegedly failed to heed the government's warning and for years engaged in what a former Georgia Tech employee called "no enforcement" of cybersecurity regulations. Georgia Tech purportedly bowed to the pressures of large dollar grant recipient researchers who pushed back on cybersecurity compliance because of what they saw as the excessive burdens. As opposed to a culture of compliance that DOJ repeatedly emphasizes in its corporate enforcement policies,[3]

Related People

- Nicole Engisch
- Alex Hontos
- Seth Goertz

Related Capabilities

- Government Contracts Counseling & Litigation
- Government Enforcement & Corporate Investigations
- Higher Education & Academic Research Institutions
- Emerging Companies
- Privacy & Social Media

Georgia Tech allegedly failed to comply with these cybersecurity requirements. More specifically, a lab at Georgia Tech allegedly failed to develop or implement a required system security plan to outline how the lab would protect covered defense information in its possession, and it failed to install or update antivirus software on servers and computers that contained non-public DoD information. The complaint alleges that Georgia Tech violated the DoD contractual conditions by failing to provide DoD with an accurate summary level score to demonstrate the lab's compliance with applicable cybersecurity regulations. Instead, Georgia Tech allegedly provided DoD with a false summary score for a "campus-wide" IT system when purportedly no such system existed.

The complaint's primary cause of action is not for breach of contract or an administrative sanction; it is the False Claims Act, 31 U.S.C. §§ 3729–3733. The False Claims Act provides that any person who "knowingly presents, or causes to be presented, a false or fraudulent claim" to the government, or who "knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim," is liable to the federal government for significant financial penalties per false claim plus treble damages.

A Georgia Tech spokesperson issued a statement denying the allegations and noting that "in this case, there was no breach of information, and no data leaked."[4]

This is DOJ's first complaint-in-intervention in a False Claims Act filed under DOJ's Civil Cyber-Fraud Initiative (CCFI).[5] When the CCFI was first launched in October 2021, DOJ Deputy Attorney General Lisa Monaco announced that its goal was to "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."[6] DOJ said that its CCFI would rely on "the False Claims Act to pursue cybersecurity related fraud by government contractors and grant recipients."[7] Although this is the first complaint-in-intervention filed by DOJ, over the past two years, DOJ's CCFI has reached multimillion dollar settlements in several other cases.[8]

DOJ's complaint-in-intervention comes on the heels of DoD's recently announced rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) to incorporate contractual requirements related to the proposed Cybersecurity Maturity Model Certification (CMMC) 2.0 program rule.[9] The proposed rule will apply to all DoD solicitations and contracts, will require contractors to prove required CMMC compliance, and will require all contractors to self-certify or to obtain a third-party certification before beginning work on any DoD contracts.

Key Takeaways

Beyond protecting against cyber incidents, robust cybersecurity protocols are now legal requirements that the government will enforce aggressively. To minimize the risk of facing a False Claims Act case or a government investigation more broadly, research

universities and other government contractors should:

- Review compliance programs, including compliance hotlines, internal monitoring and audit functions, and employee training on these programs, to ensure that they are functioning effectively and truly foster a "culture of compliance;"
- Evaluate cybersecurity policies and practices, especially subcontractor policies and practices, to ensure compliance with federal regulations and contractual requirements, such as identifying the location of all non-public government data and ensuring implementation of appropriate and effective cybersecurity assessments and plans;
- Document their own and their subcontractors' cybersecurity protocols and use regular audits or assessments to validate and ensure that these protocols are effective, complaint with legal requirements, and working as intended;
- Ensure that business leadership and, in the case of federal grant funding, Principal Investigators, understand the consequences for non-compliance with cybersecurity requirements, including potential personal exposure;
- Verify that all reports to and communications with the government are accurate and truthful and contain no material omissions; and
- Conduct prompt, credible investigations of complaints about non-compliance and, where appropriate, provide timely voluntary self-disclosure to the United States.

[1] Office of Public Affairs | United States Files Suit Against the Georgia Institute of Technology and Georgia Tech Research Corporation Alleging Cybersecurity Violations | United States Department of Justice.

[2] The case is *U.S. ex rel. Craig and Koza v. Georgia Tech Research Corp. et al*., Civil Case No. 1:22-cv-02698 (N.D. Ga.). The complaint is available online: https://www.justice.gov/opa/media/1364901/dl?inline.

[3] Microsoft Word - 2023.03.03 - Revised ECCP (revised3) (justice.gov).

[4] Federal Gov't Hits Georgia Tech With Cybersecurity FCA Suit - Law360.

[5] Northern District of Georgia | United States Files Suit Against the Georgia Institute of Technology and Georgia Tech Research Corporation Alleging Cybersecurity Violations | United States Department of Justice.

[6] Office of Public Affairs | Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative | United States Department of Justice.

[7] Id.

[8] See Office of Public Affairs | Staffing Company to Pay $2.7M for Alleged Failure to Provide Adequate Cybersecurity for COVID-19 Contact Tracing Data | United States Department of Justice; Office of Public Affairs |Consulting Companies to Pay $11.3M for Failing to Comply with Cybersecurity Requirements in Federally Funded Contract | United States Department of Justice; Office of Public Affairs | Cooperating Federal

Contractor Resolves Liability for Alleged False Claims Caused by Failure to Fully Implement Cybersecurity Controls | United States Department of Justice; Office of Public Affairs | Aerojet Rocketdyne Agrees to Pay $9 Million to Resolve False Claims Act Allegations of Cybersecurity Violations in Federal Government Contracts | United States Department of Justice; Office of Public Affairs | Jelly Bean Communications Design and its Manager Settle False Claims Act Liability for Cybersecurity Failures on Florida Medicaid Enrollment Website | United States Department of Justice

[9] Federal Register :: Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041).