Published on *The National Law Review* https://natlawreview.com

# DOJ Sues Georgia Tech Entities for Cybersecurity Failures in the Latest Civil Cyber Fraud Initiative (CCFI) Activity

Article By:

Townsend L. Bourne

A. Joseph Jay, III

On August 22, 2024, the United States Department of Justice (DOJ) filed a Complaint-In-Intervention (the "Complaint") against the Georgia Institute of Technology (Georgia Tech) and Georgia Tech Research Corp. (GTRC). The 99-page DOJ Complaint alleges the defendants knowingly failed to meet contractual cybersecurity requirements in connection with various Department of Defense (DoD) contracts. The suit raises claims under the False Claims Act and federal common law (including fraud, negligent misrepresentation, breach of contract, unjust enrichment, and payment by mistake). This is the latest DOJ activity relating to its Civil Cyber Fraud Initiative (announced in October 2021), which we previously have written about here, here, and here.

The original whistleblower suit (captioned *United States ex rel. Craig v. Georgia Tech Research Corp, et al.*, No. 1:22-cv-02698 (N.D. Ga.)) was initiated in July 2022 by former senior members of Georgia Tech's Cybersecurity team. Following a lengthy investigation, the DOJ intervened in the case in February 2024 and the original complaint was unsealed.

Now, with the most recently filing, DOJ has filed its own complaint in the case. Among other things, the DOJ's Complaint alleges:

- Until at least February 2020, a lab at Georgia Tech failed to develop and implement a system security plan (SSP) (setting out cybersecurity controls required in the lab), which is required by DoD cybersecurity regulations.
- Even when the lab implemented a system security plan in February 2020, Georgia Tech failed to properly scope that plan to include all covered equipment (i.e., laptops, desktops, and servers).
- In December 2020 Georgia Tech and GTRC submitted a false cybersecurity assessment score to DoD for the Georgia Tech campus. DoD regulations (*i.e.*, DFARS 252.204-7020) require contractors to submit summary level scores reflecting the status of their compliance with applicable cybersecurity requirements on covered contractor information systems (*i.e.*, contractor systems that process, store, or transmit controlled unclassified information). Here, DOJ alleges the submission of a score was a "condition of contract" award and Georgia Tech and GTRC submitted a false score of 98 (a perfect score is 110).

- Until December 2021, the lab failed to install, update or run anti-virus or anti-malware tools on IT equipment at the lab. Instead, Georgia Tech specifically approved the lab's refusal to install antivirus software – in violation of Georgia Tech's policies and federal cybersecurity requirements.

While the total amount of damages remains to be seen, the Complaint specifically points to payments made by the Government under the contracts, resulting from allegedly false invoices, totaling over $19 million. Of course, with the False Claims Act's permitted penalties and treble damages, the final number could potentially be much higher. As permitted by the False Claims Act, with the intervention, DOJ will take over responsibility for litigating the case going forward.

This case will have significant implications for entities that contract with the federal government and outlines areas of focus for agencies when it comes to cybersecurity. Contractors should focus on having adequate documentation to support security assessments and plans, understanding where data is housed or transmitted within information systems in order to properly scope assessments, and ensuring any reports to the government are accurate and complete in order to limit False Claims Act risk.



National Law Review, Volume XIV, Number 236