PRESS RELEASE

United States Files Suit Against the Georgia Institute of Technology and Georgia Tech Research Corporation Alleging Cybersecurity Violations

Thursday, August 22, 2024

For Immediate Release

Office of Public Affairs

The United States joined a whistleblower suit and filed a complaint-in-intervention against the Georgia Institute of Technology (Georgia Tech) and Georgia Tech Research Corp. (GTRC) asserting claims that those defendants knowingly failed to meet cybersecurity requirements in connection with the Department of Defense (DoD) contracts. GTRC is an affiliate of Georgia Tech that contracts with government agencies for work to be performed at Georgia Tech. The whistleblower suit was initiated by current and former members of Georgia Tech's Cybersecurity team.

"Government contractors that fail to fully implement required cybersecurity controls jeopardize the confidentiality of sensitive government information," said Principal Deputy Assistant Attorney General Brian M. Boynton, head of the Justice Department's Civil Division. "The department's Civil Cyber-Fraud Initiative was designed to identify such contractors and to hold them accountable."

Specifically, the lawsuit alleges that until at least February 2020, the Astrolavos Lab at Georgia Tech failed to develop and implement a system security plan, which is required by DoD cybersecurity regulations, that set out the cybersecurity controls that Georgia Tech was

required to put in place in the lab. Even when the Astrolavos Lab finally implemented a system security plan in February 2020, the lawsuit alleges that Georgia Tech failed to properly scope that plan to include all covered laptops, desktops, and servers.

Additionally, the lawsuit alleges until December 2021, the Astrolavos lab failed to install, update or run anti-virus or anti-malware tools on desktops, laptops, servers and networks at the lab. Instead, Georgia Tech approved the lab's refusal to install antivirus software — in violation of both federal cybersecurity requirements and Georgia Tech's own policies — to satisfy the demands of the professor who headed the lab.

The lawsuit further alleges that in December 2020 Georgia Tech and GTRC submitted a false cybersecurity assessment score to DoD for the Georgia Tech campus. DoD requires contractors to submit summary level scores reflecting the status of their compliance with applicable cybersecurity requirements on covered contracting systems that are used to store or access covered defense information. The submission of this score was a "condition of contract award" for Georgia Tech's DoD contracts. The lawsuit alleges that the summary level score of 98 for the Georgia Tech campus that Georgia Tech and GTRC reported to DoD in December 2020 was false because (1) Georgia Tech did not actually have a campus-wide IT system and (2) the score was for a "fictitious" or "virtual" environment and did not apply to any covered contracting system at Georgia Tech that could or would ever process, store or transmit covered defense information.

"Cybersecurity compliance by government contractors is critical in safeguarding U.S. information and systems against threats posed by malicious actors," said U.S. Attorney Ryan K. Buchanan for the Northern District of Georgia. "For this reason, we expect contractors to abide by cybersecurity requirements in their contracts and grants, regardless of the size or type of the organization or the number of contracts involved. Our office will hold accountable those contractors who ignore cybersecurity rules."

"Deficiencies in cybersecurity controls pose a significant threat not only to our national security, but also to the safety of the men and women of our armed services who risk their lives daily," said Special Agent in Charge Darrin K. Jones of the DoD's Office of Inspector General, Defense Criminal Investigative Service (DCIS), Southeast Field Office. "As force multipliers, we place a substantial amount of trust in our contractors and expect them to meet the strict standards our service members deserve."

The whistleblower lawsuit was filed by Christopher Craig and Kyle Koza, who were previously senior members of Georgia Tech's cybersecurity compliance team, under the *qui tam* or whistleblower provisions of the False Claims Act, which allow private parties to file suit on behalf of the United States for false claims and to receive a share of any recovery. The act permits the United States to intervene and take over responsibility for litigating these cases, as

it has done here. A defendant who violates the act is subject to liability for three times the government's losses, plus applicable penalties.

On Oct. 6, 2021, Deputy Attorney General Lisa Monaco announced the department's Civil Cyber-Fraud Initiative 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. Information on how to report cyber fraud can be found here.

Senior Trial Counsel Jake M. Shields of the Justice Department's Civil Division and Assistant U.S. Attorneys Adam D. Nugent and Melanie D. Hendry for the Northern District of Georgia are handling the matter.

The case is captioned *United States ex rel. Craig v. Georgia Tech Research Corp, et al.*, No. 1:22-cv-02698 (N.D. Ga.). Investigative support is being provided by the DoD Office of Inspector General, Defense Criminal Investigative Service, Air Force Office of Special Investigations and Air Force Material Command.

The claims alleged by the United States are allegations only. There has been no determination of liability.

Complaint

Updated August 23, 2024

Topic

FALSE CLAIMS ACT

Components

Civil Division | USAO - Georgia, Northern

Press Release Number: 24-1044

Related Content

PRESS RELEASE

California Mobile Phlebotomy Lab and Its Owners to Pay $135,000 to Resolve Allegedly False Claims for Blood Testing Services and Travel Mileage

Veni-Express Inc. (Veni-Express), headquartered in California, and its owners Myrna and Sonny Steinbaum have agreed to pay at least $135,000 to resolve False Claims Act allegations that they submitted false...

October 22, 2024

PRESS RELEASE

The Pennsylvania State University Agrees to Pay $1.25M to Resolve False Claims Act Allegations Relating to Non-Compliance with Contractual Cybersecurity Requirements

The Pennsylvania State University (Penn State), located in University Park, Pennsylvania, has agreed to pay $1,250,000 to resolve allegations that it violated the False Claims Act by failing to comply...

October 22, 2024

PRESS RELEASE

Raytheon Company to Pay Over $950M in Connection with Defective Pricing, Foreign Bribery, and Export Control Schemes

Raytheon Company (Raytheon) — a subsidiary of Arlington, Virginia-based defense contractor RTX (formerly known as Raytheon Technologies Corporation) — will pay over $950 million to resolve the Justice Department's investigations into...

October 16, 2024

Office of Public Affairs

U.S. Department of Justice

950 Pennsylvania Avenue, NW

Washington DC 20530

Office of Public Affairs Direct Line

202-514-2007

Department of Justice Main Switchboard

202-514-2000