Whitepaper: Implications of Georgia Tech False Claims Act Lawsuit

On August 22, 2024 the US Department of Justice filed a False Claims Act lawsuit against Georgia Technical University for falsely claiming compliance with cybersecurity obligations. This is the first time the DOJ has joined in an FCA suit under the DOJ Civil Cyber-Fraud Initiative that was announced by Deputy Attorney General Lisa Monaco in October 2021.

Legal firm McCarter & English pointed out that "with this case pending and under investigation (as are all FCA cases before unsealing) for the past two years, there's a near 100 percent chance that this isn't the only case out there. Announced as part of the DOJ's broader effort under its Civil Cyber-Fraud Initiative, the complaint demonstrates the means by which the DOJ intends to hold contractors accountable for deficient cybersecurity practices capable of putting US information and systems at risk."

McCarter & English noted that "the amended complaint alleges that the lab submitted false cybersecurity assessment scores into the Supplier Performance Risk System (SPRS) in order to be perceived as meeting the requirements of DFARS 252-204-7019 and -7020 in December 2020. The SPRS score submitted—a 98, for those wondering—was viewed as false by the DOJ because the score was for a "fictitious" or "virtual" environment and did not apply to any actual research environment or covered contracting system. The DOJ highlighted that the purportedly fraudulent SPRS submission was crucial and a "condition of [DoD] contract award."

The legal analysis by McCarter & English is well worth reviewing. If you are wondering if you are compliant, you almost certainly are not.

A Federal News Network article commented that "Perhaps this case, in its density, is intended to combat anyone who might hold the misapprehension that DoJ is not serious about using the False Claims Act as a means not only to punish companies that it decides to pursue, but also to warn any other companies of the importance that they thoroughly understand their obligations and thoroughly perform those cyber obligations without acts that are indifferent, misleading or fraudulent,"

The original FCA filing in July of 2022 was by two "qui tam relators" (whistleblowers) named Christopher Craig and Kyle Koza. Both suffered retaliation for their complaints about non-compliance. Retaliation is strictly forbidden by the FCA.

The scope of the non-compliance is impressive. The project that triggered the original issues was known as the EA Contract. Page 81 of the DOJ filing noted

> “The Astrolavos Lab began work on the EA Contract in late 2016, and was processing, storing, or transmitting Controlled Defense Information on its information systems by May 28, 2019. Over the course of the contract, GTRC submitted approximately 43 invoices to DoD for work performed on the EA Contract, totaling $21,891,306. Each of the invoices described the services provided or goods purchased in connection with the contract. Each invoice included the following certification: “I certify that all payments are for appropriate purposes and in accordance with the agreements set forth in the application and award documents.” None of the invoices mention Georgia Tech or GTRC’s failure to comply with applicable federal cybersecurity rules and regulations. “

As the original qui tam relators Craig and Koza are eligible to receive 30% of the funds recovered by the DOJ. If the jury restricts recovery to the invoiced EA contract of $21,891,306, the relators could split $6.5 million. This far exceeds the $2.61 million awarded the relator in the $9 million dollar Aerojet Rocketdyne cybersecurity case.

The DOJ is seeking triple damages plus legal fees. On page 10 of the DOJ filing it is noted that in FY 2021 and 2022 GT conducted $1.6 billion in federal contracts, mostly with the DoD.

The description of the GT practices is truly disturbing. On page 6 of the DOJ filing, a former GT employee was quoted as stating “Georgia Tech will only comply with applicable rules such as the cybersecurity regulations at issue here “after an event has happened”—such as “getting in trouble with the government.”

Legal Issues – FCA Fines and Qui Tam Lawsuits

The FCA is a very powerful law, resulting in $billions of dollars of overcharges recovered.

Links

https://www.theregister.com/2024/08/23/us_georgia_tech_lawsuit/

https://federalnewsnetwork.com/cybersecurity/2024/08/dojs-georgia-tech-lawsuit-a-warning-to-contractors-on-cyber-compliance/

https://www.summit7.us/blog/united-states-sues-georgia-tech

GTRI Criminal case https://www.justice.gov/usao-ndga/pr/former-chief-scientist-georgia-tech-research-institute-sentenced-conspiring-defraud

Excessive FCA fine? https://www.arnoldporter.com/en/perspectives/blogs/fca-qui-notes/posts/2024/07/78-times-is-not-the-charm

https://www.omm.com/insights/alerts-publications/doj-intervention-in-cybersecurity-suit-is-a-harbinger-of-cyber-fraud-initiative-s-focus-on-contractor-information-security-practices/

Whistleblower constitutionality questions
https://www.arnoldporter.com/en/perspectives/blogs/fca-qui-notes/posts/2024/08/fca-sky-wont-fall