Title: DOJ's Civil Cyber-Fraud Initiative Settlement Shows Growing False Claims Act Risk

Brief Overview: A recent settlement between the United States Department of Justice (DOJ) and Georgia Tech Research Corporation (GTRC), a research affiliate of the Georgia Institute of Technology (Georgia Tech), shows that the DOJ remains committed to using the False Claims Act (FCA) to ensure compliance with cybersecurity measures required under federal contracts.

Companies, research organizations, and other entities that maintain sensitive data pursuant to contracts with the federal government must be sure to comply with contractual cybersecurity requirements or face the prospect of a DOJ investigation.

Learn more about the GTRC settlement, including key takeaways for those potentially impacted through actions brought in connection with the DOJ's Civil Cyber-Fraud Initiative.

Full Article: A recent settlement between the United States Department of Justice (DOJ) and Georgia Tech Research Corporation (GTRC), a research affiliate of the Georgia Institute of Technology (Georgia Tech), shows that the DOJ remains committed to using the False Claims Act (FCA) to ensure compliance with cybersecurity measures required under federal contracts. Companies, research organizations, and other entities that maintain sensitive data pursuant to contracts with the federal government must be sure to comply with contractual cybersecurity requirements or face the prospect of a DOJ investigation.

On September 30, 2025, the DOJ announced that GTRC agreed to pay $875,000 to resolve allegations that it had violated the FCA by failing to meet federal cybersecurity requirements regarding the safeguarding of data in connection with government contracts. GTRC contracts with various government agencies, including the Air Force and Defense Advanced Research Projects Agency (DARPA), to perform research at Georgia Tech.

The Government began using the FCA to identify, investigate, and enforce cybersecurity noncompliance in 2021 and has recovered millions of dollars from companies and universities across several cases since then. With cyber threats continuing to evolve, the Civil Cyber-Fraud Initiative will remain a critical tool for the Government to leverage the FCA to address and deter cybersecurity lapses affecting government information and data.

Civil Cyber-Fraud Initiative

The DOJ launched its Civil Cyber-Fraud Initiative in October 2021 to investigate and punish non-compliance with federal cybersecurity requirements. When organizations contract with the federal government and handle sensitive data, those organizations are required to certify that they have certain cybersecurity measures and certifications in place. These can and do include requirements that contracting entities submit and maintain certain cybersecurity scores and the implementation of security controls specified in National Institute of Standards and Technology Special Publication 800-171 (NIST SP 800-171). Organizations that certify compliance with these contractual measures but fail to put them in place have submitted false claims for payment to the government and could be in violation of the FCA.

Through the Civil Cyber-Fraud Initiative, the DOJ seeks to hold entities and individuals accountable for placing government information at risk by knowingly (1) providing deficient cybersecurity products or services, (2) misrepresenting their cybersecurity practices or protocols, or (3) violating obligations to monitor and report cybersecurity incidents and breaches.

Under the FCA, private parties, known as "relators" or whistleblowers, may file *qui tam* lawsuits on behalf of the Government, facilitating the identification of fraud and permitting relators to share in any recovery resulting from successful claims. To prevail in an FCA matter, the Government need not show that a defendant intended to defraud the Government, only that the defendant acted in reckless disregard of the truth or falsity of the information. It is also not a requirement that there be an actual data breach for there to be an FCA violation.

GTRC Settlement

The GTRC settlement results from an FCA *qui tam* lawsuit initiated in 2022 by former members of Georgia Tech's Cybersecurity Team. The DOJ subsequently intervened on behalf of the Department of Defense (DOD) and DARPA in 2024, alleging in its Complaint-in-Intervention that GTRC (1) failed to install antivirus tools at Georgia

Tech's Astrolavos Lab while conducting sensitive cyber-defense research linked to DARPA contracts, (2) neglected to implement a plan dictating the Lab's cybersecurity controls as required by its government contracts, and (3) submitted a false cybersecurity assessment score to the DOD. The DOJ sought damages and penalties for as much as $28 million in DOD payments to Georgia Tech under the government contracts.

One key federal cybersecurity regulation the DOJ considered material to GTRC's government contracts is the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012. Under the DFARS, contractors handling controlled unclassified information are required to use information systems that meet standards outlined in NIST SP 800-171.

The Government alleged that the federal cybersecurity regulations were material contract terms. Because GTRC submitted invoices to the Government for its work under the Air Force and DARPA contracts, while not complying with these material contractual terms, GTRC violated the FCA under the implied certification theory.

Pursuant to the parties' settlement agreement, of the $875,000 total to be paid to the United States, $437,500 is deemed restitution to be provided to the DOJ, and the whistleblowers will receive $201,250.

Key Takeaways

This settlement underscores the litigation risks associated with insufficient cybersecurity controls and highlights the DOJ's emphasis on cybersecurity enforcement.

DOD contractors and federal grantees should be conscious of the DOJ's steady emphasis on civil cyber-fraud. The DOJ noted that this settlement should "serve as a reminder" to the industry to prioritize compliance with applicable cybersecurity requirements. In particular, representatives from the DOJ, DOD, and Air Force Office of Special Investigations confirmed each agency's intent to continue pursuit and litigation of cybersecurity violations and to hold contractors accountable for inadequate cybersecurity controls and provision of false information to the government. The DOJ's decision to intervene further demonstrates that the Government is willing and eager to litigate cybersecurity fraud claims.

Accordingly, compliance professionals should invest in and ensure the security of organizational systems and sensitive data to effectively address federal funding requirements within government contracts and associated bids and minimize the risk of legal exposure. Regardless of the degree to which a regulatory requirement appears administrative or practically difficult, the Government may insist on its implementation to protect sensitive government information and data.

As the Civil Cyber-Fraud Initiative remains a DOJ enforcement priority, Buchanan's White Collar Defense, Compliance & Investigations attorneys and its Cybersecurity and Data Privacy team can provide clients with guidance on compliance with cybersecurity requirements in government contracts and FCA investigations and litigation related to cybersecurity fraud.

Author(s)' Name(s), Title(s), and Email(s):

Mark A. Kasten

Counsel

Email: mark.kasten@bipc.com

Michael G. McLaughlin

Principal, Government Relations

Cybersecurity and Data Privacy Practice Group Co-Leader

Email: michael.mclaughlin@bipc.com

Maxwell C. Ruocco

Associate

Email: maxwell.ruocco@bipc.com

Sophie J. Beeler

Associate

Email: sophie.beeler@bipc.com