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

The U.S. Intervenes in False Claims Act Qui Tam Cybersecurity Fraud Case Against Government Contractor Georgia Tech

Article By:

Tycko & Zavareei Whistleblower Practice Group

The United States has intervened in a False Claims Act qui tam case against Georgia Tech Research Corporation, Georgia Institute of Technology, and Georgia Tech Research Institute (Collectively "Georgia Tech") for violations of NIST 800-171 for failing to protect Controlled Unclassified Information (CUI). The claims were brought by two whistleblowers, Christopher Craig, a current employee of Georgia Institute of Technology, and Kyle Koza, a graduate and former employee of Georgia Institute of Technology, who provided valuable and original information to the Department of Justice which led to its intervention in the matter. Read the complaint.

Georgia Tech is party to many DOD contracts, which are subject to National Institute of Standards and Technology (NIST) compliance. These types of federal contractors are allowed access to specific DOD information but must implement "adequate security" measures to safeguard the information that is stored internally. The covered information at the center of the suit is CUI, which pertains to information created or owned by the DOD that is not classified, like patent information, certain types of sensitive government data, and information on the manufacture or purchasing of goods and services. "Adequate" safety protocols for CUI are defined at minimum as the implementation of NIST Special Publication 800-171, which defines how to protect CUI in non-federal systems. Contractors must self-report that their systems and employees comply with NIST measures and supply a System Security Plan (SSP) to detail how their IT network, hardware, software, and security procedures all comply with NIST 800-171. For any NIST requirements not met, a contractor is obligated to create a Plan of Actions and Milestones (POA&M) to set out a timeline and measures for reaching full compliance.

In June 2017, Georgia Tech sent a memo to all departments involved with CUI, reporting the measures of NIST 800-171, demonstrating their awareness of the federal security standards and the December 31, 2017, deadline for bringing all procedures under compliance. In September 2017, Georgia Tech received guidance from NIST on how to implement the NIST standards. Despite this, Georgia Tech knowingly failed to align its policies and procedures with the compliance guidelines in several ways.

Those placed in charge of determining if a lab's practices were compliant with NIST 800-171 were not qualified to assess or report on them and therefore could not produce accurate reports to the

DOD. NIST 800-171 states that the organization handling CUI must train its personnel to carry out such tasks. Furthermore, Assessors did not randomly sample system configurations for evidence of compliance as required and were instead decided by the system administrator. This evidence was often not sufficient to prove compliance. Additionally, employees tasked with ensuring compliance were also tasked with resolving issues they identified, creating conflicts of interest and violating NIST 800-171. Certain departments also bypassed malware requirements, putting government data at risk, further violating NIST 800-171.

As early as July 2018, Koza identified issues with the process of ensuring compliance, and by 2021, his boss, Craig, had realized it too. Both relators had raised their concerns with their superiors and were waived off. In 2022, Craig received a poor performance review for his attempts to shed light on the NIST violations. Soon after, Koza was forced to resign from Georgia Tech entirely. The allegations state that on top of causing the submission of false claims for government payment, Georgia Tech also retaliated against their employees for attempting to stop the unlawful actions, violating the False Claims Act on multiple fronts.

This intervention by the U.S. highlights the efforts of the DOJ's Civil Cyber-Fraud Initiative, which allows whistleblowers to play an expanded and crucial role in the government's cybersecurity strategy. The DOJ finds it incredibly important to ensure that companies – including government contractors and grantees – follow the rules to safeguard taxpayer dollars and protect sensitive government data. The Initiative seeks to hold contractors and grant recipients accountable for putting US information and its systems at risk in three different areas:

- 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.

National Law Review, Volume XIV, Number 101