December 2024

Understanding the Cybersecurity Related False Claims Act Case Against GA Tech

This research paper is provided for informational purposes only and is not intended to constitute legal advice. I am not a licensed attorney, and nothing in this document should be construed as creating an attorney-client relationship or as a substitute for professional legal counsel.

This paper was written to fulfill a graduation requirement for the University of Baltimore School of Law and represents academic research, not legal consultation. Readers are encouraged to consult a qualified attorney for legal advice regarding any specific issue or situation.

All views and opinions expressed in this paper are solely my own and do not reflect the opinions or policies of the University of Baltimore School of Law or any other organization.

By reading this paper, you acknowledge and agree to the terms of this disclaimer.

Leslie Weinstein
THE CYBER ADVISOR
www.the-cyberadvisor.com

In August 2024, the Department of Justice (DOJ) filed its Complaint-in-Intervention against Department of Defense (DoD) contractor Georgia Institute of Technology (Georgia Tech) and Georgia Tech Research Corp. (GTRC), collectively referred to as "GA Tech" for alleged violations of the False Claims Act (FCA). The DOJ alleges that GA Tech violated multiple sections of the Defense Federal Acquisition Regulation Supplement (DFARS) by failing to implement required cybersecurity controls. *United States of America Ex Rel. Christopher Craig and Kyle Koza v. Georgia Tech Research Corp. and Board of Regents of The University System of Georgia (D/B/A The Georgia Institute of Technology)*. In October 2024, GA Tech filed a Motion to Dismiss, claiming DOJ failed to state a claim for which relief could be granted, and for failure to plead fraud with particularity. GA Tech Mot., at 1. As one of only three unsealed FCA cases involving alleged DFARS cybersecurity violations, this case lacks binding or persuasive precedent specific to the issue of cybersecurity requirements.[1] However, there is ample binding precedent to suggest that the Court is likely to find DOJ has alleged fraud with sufficient particularity to overcome GA Tech's motion to dismiss. To attach liability under the FCA and prevail on the merits of the case, the DOJ will need to prove the allegations against GA Tech and additionally show that the violations were material to the DoD.

Background

The research lab at the center of this False Claims Act suit is Georgia Tech's Center for Cyber Operations Enquiry and Unconventional Sensing (COEUS), formerly known as the Astrolavos Lab.[2] COEUS brings together academia, industry, and government to address the

[1] *United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, settled in August 2022. *United States ex rel. Decker v. Pennsylvania State University*, settled in October 2024.

[2] The DOJ complaint names Astrolavos Lab in the complaint, however, the Astrolavos Lab website now describes the lab as the Center for Cyber Operations Enquiry and Unconventional Sensing (COEUS).

security of emerging technologies critical to national security. Center for Cyber Operations Enquiry and Unconventional Sensing (COEUS), https://astrolavos.gatech.edu/ (last visited Nov 2, 2024). In its Complaint-in-Intervention, filed on August 22, 2024, the DOJ alleges that for several years COEUS received or created CUI under DoD contracts and that COEUS failed to provide "adequate security" to that CUI in violation of the DFARS 7012 clause. DOJ Compl. ¶ 152. DOJ additionally alleges that GA Tech submitted a patently false NIST 800-171 summary level score in violation of DFARS clause 7019. *Id*., at ¶ 199. DOJ asserts that GA Tech and COEUS's violations of the DFARS 7012 and 7019 clauses were material and therefore caused the United States to "pay monies to GTRC to which it was not entitled, thereby damaging the United States," in violation of the False Claims Act. 31 U.S.C § 3729(a)(1)(A)-(B). DOJ Compl. ¶ 304.

GA Tech's primary defense against these allegations is that COEUS did not handle CUI under DoD contracts, and therefore the DFARS 7012 and 7019 clauses did not apply. GA Tech Mot., at 4. As a legal matter, it is undecided whether the lab actually received or created CUI is dispositive to liability, given that the applicable provisions are indisputably part of the contracts at issue. However, as a factual matter, through the CUI Inquiry performed in section D below, it can be reasonably determined that COEUS handled multiple types of CUI under two DoD contracts. It can also be reasonably determined based on the DoD's own statements that cybersecurity requirements are material to the DoD, such that liability under the FCA may attach.

A. False Claims Act

The Department of Justice alleges that by violating specific provisions of the DFARS, GA Tech has violated the False Claims Act, 31 U.S.C. § 3729 (a)(1)(A)-(B). The False Claims Act (FCA) imposes two kinds of liability: (1) on anyone who knowingly makes, or causes someone else to make, a false claim for payment from the Government, 31 U.S.C. § 3729 (a)(1)(A), and (2) on anyone who knowingly makes, uses, or causes others to make or use materially false records to support a false claim. 31 U.S.C. § 3729 (a)(1)(B). Because Congress did not define "false" or "fraudulent" in the FCA, courts have long held that Congress intends to incorporate the well-settled common law meaning of "false" and "fraudulent" into the FCA. *Universal Health Servs.*, at 187. Common-law fraud encompasses misrepresentation by omission, and therefore misrepresentation by omission can give rise to liability under the FCA. *Universal Health Servs.*, at 187. Misrepresentation by omission may give rise to a claim under the FCA under the "implied false certification" theory. The "implied false certification theory" holds that when a contractor submits a claim for payment, the contractor is impliedly certifying compliance with all conditions of payment. Liability under the FCA may also attach for violating other material requirements of the contract that are not expressly designated as a condition of payment, and conversely, not all violations of the conditions of payment give rise to liability. *Universal Health Servs*., at 181. What gives rise to liability under the "false certification theory" is not the label that the government attaches to a requirement, but the materiality of the violation and the failure of the contractor to disclose that material violation to the government. *Universal Health Servs*, at 180. Failing to disclose a material violation renders the contractor's claim "false or fraudulent" under the FCA. *Universal Health Servs*, at 180.

However, not all violations of statutory, regulatory, or contractual requirements give rise to a claim under the FCA. For liability to be actionable under the FCA, the misrepresentation must be made with scienter and must be material to the Government's decision to pay the claim. *Universal Health Servs.,* at 180. The scienter requirement of the FCA may be met in three ways: if the defendant has actual knowledge that the information provided to the government was false or misleading, if the defendant acted in deliberate ignorance of the truth or falsity of the information, or if the defendant acted in reckless disregard of the truth or falsity of the information. §3729(b)(1)(A). The materiality requirement looks at the effect that the misrepresentation may have had on the contracting officer's decision to pay, and not just that the government would have the option to decline payment if it knew of the defendant's noncompliance. *Universal Health Servs.,* at 194. Additionally, there is strong evidence that a particular requirement is not material if the government routinely pays claims despite actual knowledge that contractors have violated that requirement. *Universal Health Servs*., at 195.

B. Cybersecurity Requirements Under the DFARS

The Defense Federal Acquisition Regulation Supplement (DFARS), 48 C.F.R. § 252 Part 204, clauses 7012 and 7019 contain the relevant cybersecurity compliance requirements at issue in this case.[3] In 2015, the DoD updated the DFARS 7012 clause to establish the minimum cybersecurity requirements that defense contractors must meet to ensure "adequate security" is provided to contractor-owned or managed information systems that handle, process, or store the sensitive but unclassified defense information that has been designated as controlled unclassified information (CUI).[4] All DoD solicitations for the acquisition of commercial products and commercial services, except those for purely commercial off-the-shelf (COTS) items, are required to include DFARS clauses 7012 and 7019. 48 C.F.R. Subpart 204.73. CUI is information that is created by, for, or on behalf of the Executive Branch for which a law,

[3] The DOJ complaint against GA Tech alleges violations of DFARS clauses 7302 and 7008 in addition to violating the DFARS 7012 clause, however, because clauses 7302 and 7008 require contractors to implement the cybersecurity requirements at DFARS clause 7012, the requirements of DFARS 7012 necessarily incorporate DFARS clause 7302 and 7008 and will not be separately reviewed.

[4] The DFARS clauses require "adequate security" for "covered defense information" (CDI), however, CDI is defined as CUI as per 32 C.F.R. Part 2002. This paper refers to all CDI as CUI.

regulation, or other government-wide policy requires the information to be protected with safeguarding or dissemination controls. 32 CFR 2002.4(h). The CUI Program was established by Executive Order 13556 in 2010 by the National Archives and Records Administration (NARA) serving as the program's Executive Agent. NARA created the CUI program through 32 C.F.R. Part 2002 in 2016, which established a consistent methodology for agencies to designate, safeguard, disseminate, mark, decontrol, and dispose of CUI. Through 32 C.F.R. Part 20023, NARA also established NIST SP 800-171 as the minimum standard for protecting CUI in non-federal information systems. *Id*., at § 2002.14. NARA also requires agencies to establish specific CUI handling requirements through written agreements with contractors when a contract involves the handling of CUI, which must include the requirement that contractors implement NIST 800-171 security controls. 32 C.F.R. § 2002.4(c) and 2002.14(h)(2).

In exigent circumstances, agency heads or the agency-designated senior CUI official may waive CUI safeguarding requirements for CUI when agencies share the CUI with contractors. *Id*., at § 2002.8(c). All CUI safeguard waivers must be documented along with the alternate protection methods the agency will employ to ensure that CUI remains properly protected. *Id*., at § 2002.8(d)(5). When the exigent circumstances that necessitated the suspension of CUI requirements end, agencies must reinstate the CUI requirements. *Id*., at § 2002.8(d)(5).

The DFARS 7012 clause is mandated for inclusion in all DoD contracts "for the acquisition of commercial products and commercial services, except for solicitations and contracts solely for the acquisition of COTS [Commercial-off-the-Shelf] items." DFARS 204.7304(c). However, if the performance of the contract does not require the contractor to handle CUI at all, or if the contractor does not handle CUI on the contractor's information system, the requirements in DFARS 7012 do not apply. Cybersecurity FAQs, DoD Procurement Toolbox.

https://dodprocurementtoolbox.com/faqs/cybersecurity/cybersecurity (last visited Nov. 28, 2024). The DoD has not provided official guidance on the applicability of the DFARS 7019 clause when the requirements of the DFARS 7012 do not apply; however, the text of the DFARS 7019 predicates its applicability on the applicability of the contractor's requirement to implement NIST 800-171, stating "[i]order to be considered for award, if the Offeror is required to implement NIST SP 800–171, the Offeror shall…" DFARS 252.204-7019(b). It stands to reason that the DoD would most likely advise that the DFARS 7019 clause does not apply if the DFARS 7012 clause does not apply.

The DFARS 7012 clause serves as the bedrock of cybersecurity-related compliance requirements upon which the DFARS 7019 clause rests. The DFARS 7019 clause does not add any new cybersecurity requirements and applies only when a contractor handles CUI and is required to implement NIST 800-171 security controls. The DFARS 7019 clause establishes a bespoke methodology for assessing compliance with NIST 800-171 and provides the process by which contractors are to report their assessment results to the DoD. 48 C.F.R. § 252.204-7019(b). Contractors are also required to provide their summary level score to the DoD at least once every three years by posting the score in the DoD's Supplier Performance Risk System (SPRS). 48 C.F.R. § 252.204-7019(b). In addition to providing the summary level score, contractors must also provide a description of the information system's architecture covered by the assessment score, if the contractor has more than one relevant system, and provide a date that the contractor anticipates achieving the maximum assessment score. 48 C.F.R. § 252.204-7019(d)(1).

Before contract award or to exercising an option period or extending the period of performance of an existing contract, DoD contracting officers are required to verify that a contractor has a summary level score in SPRS for each relevant contractor information system that handles or protects CUI. DFARS Subpart 204.7303. There is no guidance in the DFARS relating to a minimum or a recommended range of NIST 800-171 summary level scores.

i. NIST 800-171 Security Requirements

If compromised, CUI has the same potential for adverse impact whether it resides on a federal or contractor information system; therefore, NIST 800-171 contains the same fundamental and supplemental security requirements for protecting CUI as federal information systems. NIST 800-171, Revision 2, 6. Entitled "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," NIST 800-171 contains 110 discrete security requirements that, at a minimum, are required to provide adequate security to CUI. 32 CFR 2002.14(h)(2). As part of demonstrating NIST 800-171 compliance, contractors must document how each of the 110 security requirements has been implemented in a formalized document called a System Security Plan (SSP). NIST 800-171, 9. The SSP must also describe the system's boundary, operational environment, and relationships between the contractor's system and external systems. *Id.*, 9. For any security controls that have not yet been implemented, contractors are required to document when and how the control requirement will be implemented, and then make genuine progress toward implementation. *Id.*, 9. If contractors are unable to implement any of the NIST 800-171 control requirements, contractors may implement alternative, but equally effective, security measures that are based upon or derived from other existing and recognized security standards and controls, like NIST 800-53 or International Standards Organization (ISO) 27001. *Id.*, 9 and footnote 21.

Contractors are permitted to choose their solutions for meeting the security requirements from NIST 800-171. For example, security requirement 3.14.2 mandates that organizations provide protection from malicious code at designated locations within the contractor's system.

There are a variety of technologies and mechanisms available to limit or eliminate the effects of malicious code within a system, and include, but are not limited to, anti-virus signature definitions, reputation-based technologies, software integrity controls, and pervasive configuration management. NIST 800-171, 3.14.2, Discussion. Contractors may also choose where to implement these mechanisms within the system, such as at system entry and exit points, workstations, electronic mail servers, and mobile devices. *Id*., 3.14.2, Discussion. NIST 800-171 does not proscribe how and where malicious code protections are to be implemented; NIST 800-171 only mandates that organizations implement protections from malicious code and that the method and placement of the malicious code protections are described in the SSP.

ii. DoD's NIST 800-171 Assessment Methodology

The DoD requires contractors to use the assessment process proscribed in NIST 800-171A, "Assessing Security Requirements for Controlled Unclassified Information" to conduct NIST 800-171 assessments. NIST 800-171A is a companion publication to NIST 800-171 and provides general guidance for how to generate sufficient artifacts and evidence to evaluate the implementation of NIST 800-171's security requirements. The DoD also created a proprietary scoring procedure that contractors must use in conjunction with NIST 800-171A to generate a summary level score which provides an objective evaluation of a contractor's NIST 800-171 implementation status.[5] DoD Assessment Methodology, 5. Once the summary level score is generated, contractors are required by the DFARS 7019 clause to report the score through the

[5] A link to the current NIST SP 800-171 DoD Assessment Methodology can be found in the text of the DFARS 7019 and 7020 clauses. https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/NIST-SP-800-171-Assessment-Methodology-Version-1.2.1-6.24.2020.pdf

Supplier Performance Risk System (SPRS) to be eligible for contract award for solicitations containing the DFARS 7012 and 7019 clauses.

Assessments can be performed by the contractor as a self-assessment, by a private third-party assessor, or by a government assessment team. Regardless of the party performing the evaluation, the procedures and methods for performing a NIST 800-171 assessment are the same. Because the DoD's scoring methodology is based on a review of a contractor's descriptions of security control implementation in the SSP, it is not possible to begin a NIST 800-171 assessment if the contractor does not have a documented SSP. DoD Assessment Methodology, 7. NIST 800-171A provides at least one if not several, assessment objectives for each security requirement within NIST 800-171. There are more than 300 individual assessment objectives, and each one aligns directly with a security requirement. Each of the security objectives for a security requirement must be achieved to count the security requirement as being fully implemented. To determine if security objectives have been achieved, assessors must first review the SSP's description of the security control implementation and then gather evidence of implementation through various methods, including interviewing employees, testing technical configurations, and examining documentation.

The summary level score of a DoD NIST 800-171 assessment can range from a perfect score of 110 to a low of -203.[6] Each organization starts with a perfect score of 110 because there are 110 unique security requirements in NIST 800-171. Each security control is assigned a point

[6] The DoD's NIST 800-171 assessment methodology is based on an assessment of NIST 800-171, Revision 2. The score generated by the DoD NIST 800-171 assessment methodology is proprietary to the DoD. While the DoD assessment methodology incorporates the assessment methodology of NIST 800-171A, the point value assigned to each NIST control is used only for DoD NIST assessments. https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/NIST-SP-800-171-Assessment-Methodology-Version-1.2.1-6.24.2020.pdf

value ranging from one to five. If a control is not fully implemented, the control's corresponding points will be deducted from the total score. A score less than 110 points is, therefore, a representation that the organization has not fully implemented the NIST 800-171 security requirements.

C. GA Tech Handled CUI Under Two DoD Contracts

The DOJ alleges that GA Tech violated the False Claims Act by failing to provide adequate security to CUI, and specifically failed to provide adequate security under the "EA" and "SMOKE" contracts. GA Tech allegedly handled CUI as part of the EA contract as early as December 2016, yet GA Tech failed to develop, implement, and maintain a System Security Plan (SSP) before December 31, 2016, as required by NIST 800-171 and the DFARS 7012 clause. DOJ Compl. ¶ 152. GA Tech also failed to provide adequate security to CUI by not installing and running antivirus and incident detection software throughout the COEUS laboratory. *Id.*, ¶ 152. The DOJ additionally alleges that GA Tech was ineligible for the award of the SMOKE contract entirely, because GA Tech intentionally submitted a fictitious NIST 800-171 summary level score for a virtual environment that did not exist, in violation of the DFARS 7019 clause. *Id.*, 153, 154.

i. The "EA" Contract

From December 2016 through the end of 2021, COEUS performed work on the Air Force contract titled "Rhamnousia: Attributing Cyber Actors Through Tensor Decomposition" ("EA"). Under the EA contract, COEUS worked with the Air Force and the Defense Advanced Research (DARPA) to develop "enhanced attribution technology" that would enable the Air Force to better identify malicious cyber actors. DOJ Compl. ¶ 104. The EA solicitation plainly stated that the

DFARS 7012 clause would apply to the EA contract, as well as to all “FAR-based” awards resulting from the EA solicitation. *Id*., 106. The EA contract award letter sent from the Air Force to COEUS stated that COEUS’s offer represented to the Air Force that COEUS would comply with the NIST 800-171 security requirements no later than December 31, 2017. *Id*., 111. The award letter further stated that COEUS was to reply to the provision in the award letter regarding NIST 800-171 compliance only if COEUS needed more time to implement the security controls, or if COEUS was planning to propose a deviation from the NIST 800-171 security requirements. *Id*., 112. The DOJ complaint does not specify if, or how, COEUS replied to the NIST 800-171 compliance provision of the award letter.

As the solicitation forewarned, the EA contract incorporated the full text of the DFARS 7012 clause. The EA contract’s associated Contract Security Classification Specification (standard Department of Defense (DD) Form 254) indicated that COEUS would receive both classified and unclassified information, including unclassified information that was “For Official Use Only” (FOUO). The Security Classification Guide (CG) that accompanied the EA contract designated specific information relating to the “technical details of specific, persistent vulnerabilities of system under development” as FOUO. *Id*., 118. The CG and other EA contract materials lacked explicit references to CUI because the DoD did not publish its CUI Program policy until March 6, 2020, more than three years after COEUS began work on the EA contract. DoD Instruction (DoDI) 5200.48, Controlled Unclassified Information (CUI) (Mar 2020). The DoD CUI Program policy states that unclassified information that was marked with legacy markings, such as "FOUO," before the establishment of the CUI Program does not automatically become CUI, because only information that qualifies as CUI may be so designated. DoDI 5200.48, para. 3.2(b) and 23 C.F.R. Part 2002.4(cc). However, the lack of a CUI marking, or the presence of a legacy marking, on information that qualifies as CUI does not exempt the holder from CUI safeguarding requirements. 23 C.F.R. Part 2002.20(7).

The EA contract additionally stipulated that the items delivered under the EA contract were being developed for both civil and military applications, and therefore export controls would be applied. DOJ Compl. ¶ 109. The Export Administration Regulations (EAR) controls items that have both civil and military applications, which are often referred to as "dual-use" items. 15 C.F.R. § 734.3. The EAR supports national security by restricting access to dual-use items by those who intend to use such items against the United States. *Id.*, at § 730.6.

The EA's Contract Data Requirements also indicated that "Distribution Statement F" would apply to information under the EA contract. DOJ Compl. ¶ 113. At the time the EA contract was signed, the DoD's guidance for the applicability of Distribution Statement F was that it could only be applied to classified and unclassified information under "rare and exceptional" circumstances when a specific authority existed, or when the information could only be shared on a "need-to-know" basis. DoD Instruction (DoDI) 5230.24, Change 1, 04/28/2016, Enclosure 4(f). The Classification Guide described the classified and unclassified technical information involved in the EA contract as "scientific, technological, or economic matters relating to national security." DOJ Compl. ¶ 119.

ii. The "SMOKE" Contract

COEUS began performing work on the Signature Management using Operational Knowledge and Environments (SMOKE) contract, officially titled "Antikythera: A Novel Framework to Assess, Statistically Model and Evade CYB," in October 2022. The goal of the SMOKE program is to develop "signature management technologies that generate evasive cyber infrastructure by incorporating counter-attribution techniques into the design process…and eliminate signatures as a source of attribution." DARPA, Broad Agency Announcement Signature Management using Operational Knowledge and Environments (SMOKE)[7]. In the context of cybersecurity, a "signature" is an observable and distinguishable pattern of behavior in cyberspace that can be used to trace the origin of an action and is most often used to identify threats in an environment. NIST 800-61, Revision 2, Appendix C-Glossary. DARPA anticipates the deliverables of the SMOKE contract will help DoD cyber planners assess attribution risks associated with infrastructure decisions and recommend infrastructure configurations to minimize those risks to acceptable levels. SMOKE Proposer's Day, Exemplary SMOKE Use Cases. Cyberspace operations when the intent is that the activity or operation will not be apparent or acknowledged publicly is a "clandestine military activity or operation in cyberspace," and are marked by secrecy. 10 U.S. Code § 394(c) and (f)(1)(A).

The SMOKE project requires GA Tech to engage in iterative development cycles, which requires multiple rounds of incremental capabilities development that are delivered as "operational prototypes," and which must be further tested and evaluated by military end-users on the same platforms that are used to conduct military cyber operations. SMOKE Proposer's Day, Transition Support Activity. Therefore, GA Tech researchers are necessarily required to receive military end-user testing and evaluation data. Although the original statement of work (SOW) included only fundamental research tasks, the original Contract Security Classification Specification (DD Form 254) expressly notified GA Tech that CUI would be handled as part of the SMOKE contract. DOJ Compl. ¶ 130. And even before the contract began, COEUS requested

[7] https://sam.gov/api/prod/opps/v3/opportunities/resources/files/cc680f6b10a148209edc7aaa992565cf/download?&status=archived&token=

access to CUI which prompted DARPA to modify the SOW shortly after the contract was executed to include non-fundamental research tasks. *Id*., 128.

In addition to minimizing DoD signature emissions, the SMOKE contract contemplates using contract deliverables to "accelerate red team cyber security assessments of DoD networks" by automatically generating attack plans and infrastructures that mimic known advanced cyber threats. SMOKE Proposer's Day, Exemplary SMOKE Use Cases. To iterate on deliverables for this specific use case, GA Tech would necessarily be required to receive test and evaluation data relating to cybersecurity assessments of DoD infrastructure.

D. Assessing Georgia Tech's Liability Under the False Claims Act

To establish COEUS's liability under the False Claims Act for violations of DFARS clause 7012 in this case, DOJ must (1) prove that COEUS created, processed, or stored controlled unclassified information (CUI); (2) prove that COEUS knowingly failed to provide adequate security to CUI by its failure to implement NIST 800-171, and (3) that COEUS's failure to provide adequate security to CUI would have had a natural tendency to influence, or be capable of influencing, the Government's decision to pay GA Tech. 31 U.S.C § 3729 (b)(4).

To establish liability under the False Claims Act for alleged violations of the DFARS 7019 clause, DOJ must (1) prove that COEUS handled CUI and therefore the assessment and reporting requirements in the DFARS 7019 clause applied, (2) prove that GA Tech's NIST 800-171 summary level score was not based upon a legitimate self-assessment which included COEUS information system that handled, processed, and stored CUI; and (3) prove that GA Tech's NIST 800-171 summary level score was both fraudulent and material to the Government's decision to award contracts to GA Tech. 31 U.S.C § 3729 (b)(4).

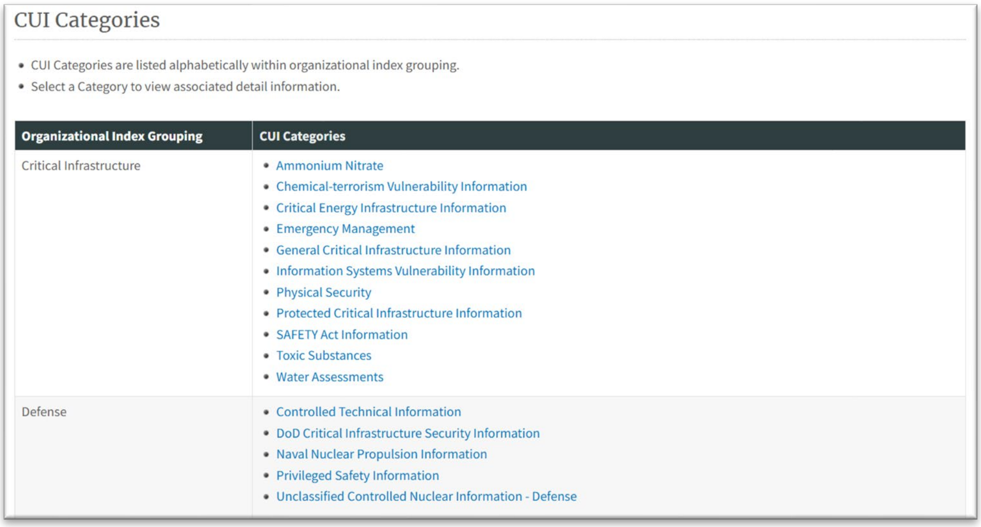
While the nuance of proving liability under the FCA for violations of the DFARS 7012 clause varies slightly from proving liability for violations of the DFARS 7019 clause, the DOJ must ultimately prove the same main elements to establish liability under the FCA. To establish liability under the FCA, DOJ must prove that (1) COEUS handled CUI, such that COEUS was subject to the requirements of the DFARS 7012 and 7019 clauses, (2) COEUS knowingly did not comply with the requirements of DFARS 7012 and 7019 clauses, and that (3) COEUS's violations of the DFARS clauses would have had a natural tendency to influence, or be capable of influencing, the Government's decision to award GA Tech a DoD contract, or to pay GA Tech's invoices under the contract. 31 U.S.C § 3729 (b)(4).

1) COEUS Handled CUI Under Two DoD Contracts

Due to the involvement of classified information, there is no question that COEUS handled sensitive unclassified information under the EA and SMOKE contracts. However, to determine if the unclassified information handled by COEUS under these contracts qualifies as CUI, there must be a CUI inquiry to determine if the sensitive but unclassified information could reasonably be designated as CUI. Designating unclassified information types as CUI requires that the information type fits into at least one of the categories of CUI in the CUI registry, because only information that falls into a CUI category may be designated as CUI. 32 CFR 2002.4(k). The CUI inquiry is like the process that authorized holders of CUI must follow to designate information they create as CUI.

The CUI Inquiry

The first step in the CUI inquiry is to consider the list of CUI categories in the CUI Registry and determine which categories of CUI, if any, the specific information in question could reasonably fall into. There are more than 100 categories of CUI in the CUI Registry and information may fall into more than one category of CUI. Based on the nature of the EA contract itself, the applicability of export controls, and Distribution Statement F, the EA contract's unclassified information could reasonably fall into the Controlled Technical Information (CTI), Export Controlled Research (EXPTR), Export Controlled (EXPT), and General Intelligence (INTEL) categories of CUI. Due to the clandestine nature of the contract's deliverables and the deliverables' ability to conduct assessments of DoD networks, the information handled by GA under the SMOKE contract could reasonably fall into the CTI, INTEL, and Information Systems Vulnerability Information (ISVI) categories of CUI.



CUI Categories

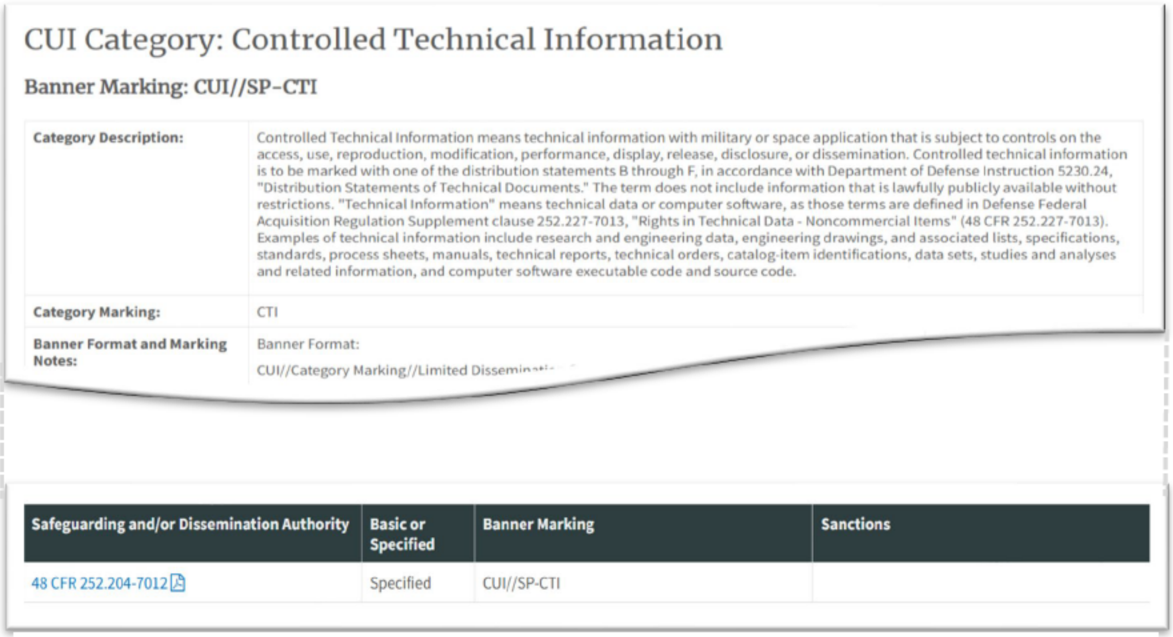
- CUI Categories are listed alphabetically within organizational index grouping.
- Select a Category to view associated detail information.

Organizational Index Grouping	CUI Categories
Critical Infrastructure	• Ammonium Nitrate • Chemical-terrorism Vulnerability Information • Critical Energy Infrastructure Information • Emergency Management • General Critical Infrastructure Information • Information Systems Vulnerability Information • Physical Security • Protected Critical Infrastructure Information • SAFETY Act Information • Toxic Substances • Water Assessments
Defense	• Controlled Technical Information • DoD Critical Infrastructure Security Information • Naval Nuclear Propulsion Information • Privileged Safety Information • Unclassified Controlled Nuclear Information - Defense

Figure 1 The CUI Registry provides the only authoritative list of CUI categories

https://www.archives.gov/cui/registry/category-list

The second step in the CUI inquiry is to carefully read the NARA-provided definitions of each of the CUI categories identified as potential matches to the information in question to determine if the information in question falls within the scope of the definition. If the NARA definition is insufficient to make a designation determination, NARA provides links to the associated laws, regulations, and other government-wide policies that were used to designate the information type as CUI which may provide clarifying information to make the determination.



CUI Category: Controlled Technical Information

Banner Marking: CUI//SP-CTI

Category Description:	Controlled Technical Information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information is to be marked with one of the distribution statements B through F, in accordance with Department of Defense Instruction 5230.24, "Distribution Statements of Technical Documents." The term does not include information that is lawfully publicly available without restrictions. "Technical Information" means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data - Noncommercial Items" (48 CFR 252.227-7013). Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.
Category Marking:	CTI
Banner Format and Marking Notes:	Banner Format: CUI//Category Marking//Limited Dissemin

Safeguarding and/or Dissemination Authority	Basic or Specified	Banner Marking	Sanctions
48 CFR 252.204-7012	Specified	CUI//SP-CTI	

Figure 2: NARA Definition of CUI Category and the CUI Designation Authority
https://www.archives.gov/cui/registry/category-detail/controlled-technical-info.html

Individuals, agencies, organizations, and other groups of users that are authorized to handle CUI are also authorized to designate information that qualifies CUI as CUI. 32 CFR 2002.4(d). When new information is generated, or when information is received without any markings at all, authorized holders of CUI are responsible for designating the information as CUI if it qualifies as CUI. *Id*., 2002.4(t). Similarly, the third and final step in the CUI inquiry is to conclude that the information type in question could reasonably be designated as CUI, or that the information type could not be so designated because it falls outside the scope of all CUI categories.

CUI Inquiry for Controlled Technical Information (CTI)

Controlled Technical Information (CTI) is the most obvious category of CUI that COEUS handled under the EA contract. There are no allegations by the DOJ that COEUS handled CTI under the SMOKE contract. CTI is technical information, including research data, which has military application and must be marked with one of the distribution statements B through F. CUI Registry, https://www.archives.gov/cui/registry/category-detail/controlled-technical-info.html (last visited Nov 2, 2024). DoD contracts are required to notify contractors if the contractor will receive, produce, or otherwise handle CTI in the performance of the DoD contract. DFARS 7012(a)(1)-(2).

The EA contract explicitly stated that the EA program involved military applications, and that Distribution Statement F would apply. All unclassified technical information relating to the items with military applications would most likely be designated as CTI.

CUI Inquiry for Export Controlled Research (EXPTR)

Export Controlled Research (EXPTR) is the second category of CUI that the information COEUS received or produced under the EA contract could fall into. There are no allegations made by the DOJ that COEUS handled EXPTR under the SMOKE contract. EXPTR includes software that arises during, or results from, fundamental research, and that is intended to be published by the researchers, once all Government-imposed national security controls have been fulfilled. CUI Registry, https://www.archives.gov/cui/registry/category-detail/export-controlled-research (last visited Nov 2, 2024) and 15 C.F.R. § 734.8(b) and Note 3 to paragraph (b). The results of fundamental research are ordinarily published and shared widely, and therefore may never be designated as CUI. 48 C.F.R. 252.204-7000(a)(3). Not only may fundamental research never be designated as CUI, but software and other information that arises from fundamental research is not subject to the export controls of the EAR. 15 CFR 734.3(b)(3)(ii). Contracting officers may determine that all or a specified portion of a research project is "fundamental research," however, the contracting officer must document that determination, and the determination must be included in the contract. Defense Federal Acquisition Regulation Supplement (DFARS) Procedures, Guidance, and Information (PGI) 204.403(2)(i).

However, the EA contract does not contain any mention of "fundamental research," nor does it refer to the fundamental research budget activities defined by the DoD. EA Contract, Contract Number FA8750-17-C-0016 and Dep't of Defense, Fundamental Research Memorandum, Dated May 24, 2010. If the contracting officer had determined that the EA contract involved fundamental research, the contracting officer ought to have documented that determination in the EA contract. Because the EA contract lacks any mention of fundamental research, the EXPTR category of CUI most likely does not apply to the EA contract.

CUI Inquiry for Export Controlled (EXPT)

The third category of CUI that the information handled by COEUS could reasonably fall within is Export Controlled (EXPT). The EXPT category includes information relating to unclassified "dual use" software whose export could reasonably be expected to adversely impact the national security of the United States. CUI Registry, EXPT. The EA contract explicitly states that the EA program involved export controls due to the dual use of the items to be delivered under the contract. DOJ Compl. ¶ 109. Therefore, any unclassified information relating to the dual-use items under the EA contract would most certainly be designated as EXPT.

CUI Inquiry for General Intelligence (INTEL)

The fourth category of CUI that COEUS potentially handled is General Intelligence (INTEL). The information handled under both the EA and SMOKE contracts could reasonably fall within the scope of the INTEL category. INTEL information is anything related to intelligence activities, sources, and methods. CUI Registry, INTEL. Intelligence is any information that is gathered, either inside or outside the U.S., which involves threats to the nation and its interests. Dir. Of Nat'l Sec. (DNI), What is Intelligence? https://www.dni.gov/index.php/what-we-do/what-is-intelligence (last visited Nov 6, 2024). The intelligence cycle is the process by which intelligence is collected, analyzed, and developed into intelligence products for use by the intelligence community (IC). *Id*., Types of Intelligence. The goal of the EA contract was to develop "enhanced attribution technologies" to allow the Air Force to identify threat actors behind cyberattacks. DOJ Compl. ¶ 104. An attribute in cyberspace is a distinct characteristic of an object or actor, which can include a cyber actor's geographic location, a type of device (i.e., a computer or a phone), the operating system of a device, and a device's network address. NIST SP 800-95, Guide to Secure Web Services (Aug 2007). Similarly, the SMOKE contract involved the collection and analysis of signature patterns collected using cyber sensors.

The Air Force's Intelligence, Surveillance, and Reconnaissance (USAF ISR) Enterprise creates finished intelligence products for use by the IC, including other parts of the IC that fall within the DoD, which are derived from intelligence collected by cyberspace sensors. DNI, Members of the IC, https://www.dni.gov/index.php/what-we-do/members-of-the-ic?highlight=WyJzIiwiJ3MiXQ== (last visited Nov 6, 2024). The use of cyberspace sensors to collect attribution and signature data of cyber actors is a form of intelligence collection. Analyzing attribution and signature data to identify cyber actors is a form of intelligence analysis. The EA and SMOKE contracts involved the collection and analysis of cyber attribution and signature data, and therefore, the enhanced attribution technologies and signature emission data that COEUS handled or created for the Air Force and DARPA most likely relate to intelligence activities. Therefore, unclassified information handled under the EA and SMOKE contracts that relate to the Air Force attribution technologies and DARPA's signature management technology is most likely CUI and could be designated as INTEL specifically.

CUI Inquiry Conclusion: GA Tech Most Likely Handled CUI

Based on a substantive CUI inquiry and the circumstantial evidence provided in the complaint, COEUS most likely handled CUI under both the EA and SMOKE contracts such that the DFARS 7012 and 7019 clauses apply to GA Tech. GA Tech's primary defense against these allegations is that COEUS did not handle CUI under the EA and SMOKE contracts. GA Tech Mot. 4. GA Tech points to emails between COEUS, DARPA, and the Air Force that were contemporaneously exchanged with the execution of the contracts in question, in which DARPA and the Air Force allegedly confirmed that the work performed by COEUS was for fundamental research only and therefore the DFARS 7012 and 7019 did not apply. *Id*., 14. However, GA Tech fails to claim that it was the contracting officer who told COEUS that CUI would not be involved in the DoD contracts. Only contracting officers, acting within the scope of their authorities, have the authority to bind the government through administrative actions and making determinations thereto. 41 U.S.C. § 601(3) (1994). Agreements made between a contractor and the Government outside of the four corners of a government contract must be ratified by the contracting officer for the decision to be binding on the Government. *Total Med. Mgmt. v. United States*, 104 F.3d 1314, 1319 (Fed. Cir. 1997). GA Tech would have likely alleged that it was the contracting officers for the EA and SMOKE contracts who claimed that no CUI would be involved in the execution of these contracts if it had been the contracting officer who made these claims. Without ratification by the contracting officer, the Government is not bound by the assertion that CUI would not be handled by COEUS under the EA and SMOKE contracts.

2) COEUS Knowingly Violated the DFARS 7012 and 7019 Clauses

DOJ alleges that GA Tech knew, or should have known, that COEUS handled CUI under the EA and SMOKE contracts and that COEUS violated the DFARS 7012 clause by failing to implement the security requirements of NIST 800-171. DOJ additionally alleges that GA Tech failed to perform the requisite NIST 800-171 implementation assessment in accordance with the DoD's Assessment Methodology and knowingly submitted a fraudulent NIST 800-171 summary level assessment score in SPRS, in violation of the DFARS 7019 clause.

DFARS 7012 Violations

GA Tech allegedly violated the DFARS 7012 clause by failing to implement key security controls and by failing to develop, document, and update an SSP. GA Tech admits to not having a documented SSP until February 2020, more than three years after starting work on the EA contract. DOJ Compl. ¶¶ 155, 159. GA Tech notified the COEUS lab director via email in August 2019 that an SSP was required for the EA contract, which presumably spurred the development of a COEUS "lab-wide" SSP in February 2020. *Id.*, ¶¶ 159, 161. This SSP was materially noncompliant with NIST 800-171 and DFARS 7012 because the SSP excluded most of the endpoints in the COEUS lab where the research involving CUI was being conducted and the SSP has not been updated since it was created in 2020. *Id.*, ¶ ¶ 161, 171. Various employees from GA Tech have provided sworn testimony acknowledging that excluding endpoints that handle CUI from the SSP is improper and that failing to update the SSP with a defined frequency is a violation of the DFARS 7012 clause.

In mid-2023, COEUS tried again to theoretically meet the DFARS 7012 SSP requirement under the SMOKE contract by implementing a "Fundamental Research Exception SSP ("FRE

SSP")." *Id.*, ¶ 168. By his signed acceptance of the FRE SSP, the lab director at COEUS attested that no CUI would be handled by the lab as part of the SMOKE contract and that all technical deliverables would be marked as publicly releasable. *Id.*, ¶ 168. However, the COEUS lab director should have known that his FRE SSP certification was false because the SMOKE contract had been modified just nine months earlier by DARPA to explicitly add non-fundamental research tasks involving CUI to the SOW, and to add publication restrictions to the technical deliverables. *Id.*, ¶ 169. Additionally, there is no requirement within the FAR or DFARS to create an SSP for an environment that does not handle CUI.

In addition to not having a legitimate SSP, COEUS failed to implement antivirus protections at designated locations within the organizational system. Not only does NIST 800-171 require antivirus protections for CUI, but the basic safeguarding requirements for federal contract information (FCI) under the Federal Acquisition Regulation (FAR) 52.204-21 requires antivirus protections. Like CUI, FCI is non-public information generated for or on behalf of the Government to develop or deliver a product or service, but unlike CUI there are no other specific safeguarding requirements for FCI beyond the basic safeguarding requirements contained in FAR 52.204-21. In other words, any non-public information handled by a contractor that does not qualify as CUI is FCI. Regardless of whether COEUS handled CUI or not, COEUS was required to implement antivirus protections because it handed FCI.

COEUS additionally violated GA Tech's December 2017 "Controlled Unclassified Information" policy, which required anti-virus software to be installed on all endpoints that handle CUI. *Id.*, ¶ 184. GA Tech's CUI policy allowed the use of alternative and compensating controls when the installation and use of antivirus software was impractical or technically infeasible; however, this was not the case at the COEUS lab—the lab director simply did not want to install antivirus software in the lab. *Id*., ¶¶ 187-188. In December 2021, when GA Tech became aware of COEUS's failure to install antivirus software, GA Tech suspended invoicing on the EA contract due to COEUS's "non-compliance with NIST," and to "avoid a false claim." *Id*., ¶ 191. Within a few days of the invoicing suspension, the COEUS lab director allowed GA Tech's standard antivirus software to be installed throughout the COEUS lab. *Id*., ¶ 192.

There may have been additional NIST 800-171 security requirements that COEUS failed to implement, like multi-factor authentication and encrypting CUI at rest, in transit, and during use; however, without a legitimate SSP in place, it would be nearly impossible to conduct a forensic analysis of the compliance posture of the COEUS lab during the period in question.

DFARS 7019 Violations

GA Tech's alleged violations of the DFARS 7012 clause also constitute breaches of the same requirements embedded within the DFARS 7019 clause. COEUS violated the DFARS 7019 clause knowingly in two key ways. First, GA Tech failed to conduct a NIST 800-171 assessment, and second, GA Tech posted a fraudulent summary level NIST 800-171 assessment score in the Supplier Performance Risk System (SPRS).

NIST 800-171 assessments are an evaluation of the extent to which an organization has implemented each of the security requirements in NIST 800-171 and is not a value judgment about the specific approach to the implementation. DoD Assessment Methodology, 12. During the assessment process, evidence and information are gathered to determine how effective an organization's safeguards are in achieving the security requirements specified in NIST 800-171. NIST 800-171A, 1. The assessment process evaluates the efficacy of every security control by assessing each of the 300+ control objectives individually. If any of a security control's assessment objectives have not been met, then the security control must be scored as having not been fully implemented. However, the DoD Assessment Methodology strictly requires an SSP to be in place to conduct an assessment in the first place, because it is impossible to conduct a NIST 800-171 assessment without an SSP due to "incomplete information" and an inherent "noncompliance with DFARS 7012." DoD Assessment Methodology, Annex A, requirement 3.12.4. COEUS must have known they violated the DFARS 7019 when they generated a summary level score without having a legitimate SSP in place.

The summary level score of a DoD NIST 800-171 assessment provides DoD with an objective assessment of a contractor's NIST 800-171 implementation status and reflects the net effect of the security controls that have not yet been implemented. DoD Assessment Methodology, 5. In the process of submitting a summary level score in SPRS, contractors are also required to provide a brief description of the architecture covered by the NIST assessment, the date that the assessment was conducted, and the date that the contractor expects to remediate all deficiencies identified by the assessment. DFARS 7019(d)(2). Under the DoD Assessment Methodology, because COEUS failed to develop, document, and implement a legitimate NIST 800-171 SSP, COEUS could not have generated a summary level score because an assessment could not have been completed due to incomplete information and noncompliance with DFARS clause 252.204-7012. If COEUS could not have completed an assessment, then COEUS must have deliberately fabricated an assessment date and the date at which COEUS expects to implement all 110 NIST 800-171 security requirements.

3) GA Tech's DFARS Violations Were Material to the DoD's Course of Action

The DoD estimates that theft of intellectual property and sensitive information by malicious cyber actors will cost the U.S. economy between $570 billion and $1.09 trillion between 2016 and 2026. 85 FR 61505, 61518 (Sep. 29, 2020). Since 2013, the DoD has been focused on improving the cybersecurity posture of the defense industrial base by including minimum cybersecurity standards in the FAR and DFARS. *Id.*, 61518. Since 2020, the DoD has urged defense contractors to correct NIST 800-171 implementation deficiencies "immediately." *Id.*, 61518. Safeguarding CUI is such a vital requirement that the DoD will not even consider an offeror for contract award if they have not implemented NIST 800-171 and posted a summary level NIST assessment score in SPRS. *Id.*, at (c)-(d).

Liability under the FCA requires a contractor's misrepresentations to be material to the Government's course of action. *Universal Health Servs.*, at 191. The materiality standard of the FCA is demanding and requires a holistic evaluation of the likely effect a misrepresentation would have on the Government's decision to remit payment or award a contract. *Id.*, at 194 and 31 U.S.C. § 3729(b). While regulatory and contractual requirements are not automatically designated as material under the FCA, based on the DoD's statements and on-going regulatory efforts, a reasonable person would realize the significance of providing adequate security to CUI. *Id.*, at 191. GA Tech's failure to appreciate the materiality of providing basic security, let alone adequate security, to CUI amounts to "deliberate ignorance" or "reckless disregard." See *Id.*, at 191 (if a reasonable person would realize the materiality of a requirement, then the defendant should also have recognized the materiality of the requirement). A contract is "plainly illegal," and therefore void *ab initio* when it is made contrary to a regulation when the contractor knows their conduct violated the regulation. *Total Med. Mgmt. v. United States*, 104 F.3d 1314, 1319 (Fed. Cir. 1997). The Court could additionally find that the fraudulent NIST summary level score posted in SPRS induced the DoD contracting officer to award the SMOKE contract to GA Tech, and therefore could render the SMOKE contract void.

Conclusion

DOJ is likely to overcome GA Tech's Motion to Dismiss for failure to state a claim and failure to plead fraud with particularity because the evidence set forth by DOJ shows that COEUS most likely handled CUI under the EA and SMOKE contracts, triggering the applicability of DFARS 7012 and 7019. DOJ has sufficiently alleged that GA Tech knowingly failed to implement the required cybersecurity controls and submitted a fraudulent NIST 800-171 summary level score. By detailing specific instances of noncompliance and fraudulent representations, DOJ has met the heightened pleading standard for fraud under Rule 9(b), establishing a claim upon which relief can be granted.

To prevail on the merits of this case, the DOJ must prove that Georgia Tech's cybersecurity violations were material to the DoD's course of action. While the DOJ should have little difficulty demonstrating the materiality of the false NIST assessment score that GA Tech posted in SPRS to secure the SMOKE contract, a more robust analysis is necessary to evaluate the materiality of Georgia Tech's failure to implement the security requirements outlined in NIST 800-171.